Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 10 (2013) 957 – 962

Procedia Technology

International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013

Generation of AES S-Boxes with various modulus and additive constant polynomials and testing their randomization

S. Das[a], *, J.K.M.S. Uz Zaman[b], R. Ghosh[c]

[a] *Dept of Computer Science & Engg., University of Calcutta, 92 APC Road, Kolkata – 700 009, India*

[b,c] *Institute of Radio Physics & Electronics, University of Calcutta, 92 APC Road, Kolkata – 700 009, India*

Abstract

In AES, the standard S-Box is usually generated by using a particular irreducible polynomial {11B} in GF(2^8) as the modulus, with a particular additive constant {63}. In this paper, it has been shown that, by maintaining the criteria defined by Rijndael, other moduli and constants can also be used to generate different unknown S-Boxes, thus preventing linear and differential cryptanalysis. A comparative study has been made on the randomness of AES ciphertexts generated, using these S-Boxes, by the NIST Test Suite coded by us. It has been found that besides using the standard one, other modulus polynomials and additive constants are also able to generate equally or better random ciphertexts. Moreover, they can act as additional key-inputs to AES, thus increasing the key-space.

Keywords: AES S-Box; Random S-Box; NIST Test Suite; AES Additive Constant; AES Secondary Key;

. Introduction

AES, the Advanced Encryption Standard, is a substitution-cum-permutation block cipher, designed by the Belgian researchers Joan Daemen and Vincent Rijment, together called as Rijndael, reviewed and published by the National Institute of Standards and Technology (NIST), which is then approved and announced as a standard by the

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: aami.suman@gmail.com

doi:10.1016/j.protcy.2013.12.443

Federal Information Processing Standards (FIPS). In AES encryption, to introduce non-linearity, an 8-bit S-Box is generated using modular arithmetic. Based on this forward S-Box, the inverse S-Box is built for decryption [1,2,3,4].

The standard S-Box of AES is usually generated by using a particular irreducible polynomial {11B} as the modulus in GF(2^8) and a particular additive constant {63} in GF(2). Though in the original proposal of AES, Rijndael used this particular modulus and the additive constant, it has been found that other moduli and constants can also be used, making the generation of the S-Box more dynamic [5,6,7].

NIST recommended some criteria and statistical tests for characterizing the security of cryptographic algorithms. The NIST Test Suite is a statistical package of 15 tests to verify randomness of long (order of 10^6) binary sequences, which focuses on the randomness of a sequence in many ways, useful as a first step to check whether a generator is suitable for a cryptographic application. NIST also declared that statistical testing is not a substitute for cryptanalysis [8,9]. AES ciphertexts are generated with various S-Boxes and then tested to find out if the randomness as well as security varies depending on the selection of a particular S-Box.

2. Generating Various Encryption S-Boxes in AES

The AES S-Box is conventionally generated by determining the multiplicative inverses of 256 bytes (0–255), using the modulus, which are then transformed into the final substitutions as shown in eq.(1) – here the operations are in GF(2^8) and GF(2) – the inverse of zero is mapped to itself:

$$b'_i = b_i \oplus b_{(i+4)\text{mod } 8} \oplus b_{(i+5)\text{mod } 8} \oplus b_{(i+6)\text{mod } 8} \oplus b_{(i+7)\text{ mod } 8} \oplus c_i \tag{1}$$

for $0 \leq i < 8$, where b_i is the ith bit of the corresponding byte, and c_i is the ith bit of a byte c, which is an additive constant with the value {63} or 01100011. The variable b'_i is to be updated with the value on the right. In matrix form, this affine transformation can be expressed as given in eq. (2), where $[b_0,...,b_7]$ is the multiplicative inverse of the corresponding byte [5,6,7].

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{2}$$

This conventional S-Box is generated using the polynomial $m(x) = x_8 + x_4 + x_3 + x + 1$, ({11B} or 100011011) as the modulus, which is the standard S-Box described and used by Rijndael. Rows and columns of an AES S-Box are determined by the most and the least significant nibbles of each byte respectively. The modulus has been chosen from the set of 30 such polynomials of degree 8, from which Rijndael selected the first one to be used in AES. The set of irreducible polynomials in GF(2^8), that can be used to generate AES S-Boxes, is given as under [1], [4,5,6]:

11B, 11D, 12B, 12D, 139, 13F, 14D, 15F, 163, 165, 169, 171, 177, 17B, 187,
18B, 18D, 19F, 1A3, 1A9, 1B1, 1BD, 1C3, 1CF, 1D7, 1DD, 1E7, 1F3, 1F5, 1F9.

Rijndael had chosen the additive constant in such a way that the S-Box has no "fixed points" (S-Box[a]=a) and no "opposite fixed points" (S-Box[a]=a'), where a' is the bit-wise complement of a [5,6]. Depending on this logic, we extracted all valid 8-bit constants in the range {00}-{FF}, i.e., 00000000 to 11111111, those can be used as additive constants (c) in eq. (1) and (2), for the modulus {11D}, a primitive polynomial. The multiplicative inverses of the bytes in {11D} are generated with the help of the following algorithm [1]:

1. if the MSB of previous result = 0, left-shift it by one bit, else,
2. if the MSB of previous result = 1, left-shift it by one bit and XOR it with the modulus (11D) without the MSB

A list of the valid additive constants extracted is as follows:

0A, 0F, 15, 2A, 2B, 31, 32, 35, 38, 40, 4A, 4E, 54, 5E, 62, 6E, 74, 7E,
F5, F0, EA, D5, D4, CE, CD, CA, C7, BF, B5, B1, AB, A1, 9D, 91, 2B, 81.

It has also been observed that the elements in the second row of the above constants are all complements of the corresponding elements in the first row. We have generated the S-Boxes using the modulus {11D} and the above additive constants and then arbitrarily selected 8 of them for AES encryption, which encrypted a text file 300 times by using 300 same encryption keys for each S-Box, generating 300 ciphertexts for each S-Box, each ciphertext is of at least 1342500 bits, as recommended by NIST [7,8].

3. The NIST Statistical Test Suite

NIST developed a Statistical Test Suite, which is an excellent and exhaustive document consisting of 15 tests developed to test various aspects of randomness in long binary sequences produced by RNGs and PRNGs [8,9,10,11]. The tests are listed as follows:

1) *Frequency (Mono-bit) Test*: No. of 1's and 0's should be approximately the same, i.e., with probability ½.
2) *Frequency Test within a Block*: Whether frequency of 1's in an M-bit block is approximately M/2.
3) *Runs Test*: Number of runs of 1's and 0's of various lengths is as expected for a random sequence.
4) *Test for Longest-Run-of-Ones in a Block*: Whether the length of the longest run of 1's within the tested sequence (M-bit blocks) is consistent with the length of the longest run of 1's as expected.
5) *Binary Matrix Rank Test*: Checks for linear dependence among fixed length sub-strings, by finding the rank of disjoint sub-matrices of the sequence.
6) *Discrete Fourier Transform Test*: Detects periodic features in the sequence by focusing on the peak heights in the DFT of the sequence.
7) *Non-overlapping Template Matching Test*: Occurrences of a non-periodic pattern in a sequence, using a non-overlapping *m*-bit sliding window.
8) *Overlapping Template Matching Test*: Occurrences of a non-periodic pattern in a sequence, using an overlapping *m*-bit sliding window.
9) *Maurer's Universal Statistical Test*: Whether or not the sequence can be significantly compressed without loss of information, by focusing on the no. of bits between matching patterns.
10) *Linear Complexity Test*: Finds the length of a Linear Feedback Shift Register (LFSR) to generate the sequence – longer LFSRs imply better randomness.
11) *Serial Test*: Determines number of occurrences of the 2^m *m*-bit overlapping patterns across the sequence – every pattern has the same chance of appearing as of others.
12) *Approximate Entropy Test*: Compares the frequency of all possible overlapping blocks of two consecutive / adjacent lengths (m and $m + 1$).
14) *Cumulative Sums Test*: Finds whether the cumulative sum of a sequence is too large or small – focuses on maximal excursion (from 0) of random walks defined, which should be near 0.
15) *Random Excursions Test*: Finds whether number of visits to a state within a cycle deviates from expected value, calculates the number of cycles having exactly K visits in a cumulative sum random walk.
16) *Random Excursions Variant Test*: Deviations from the expected visits to various states in the random walk, calculates the number of times that a state is visited in a cumulative sum random walk.

In each test, for a bit sequence, NIST adopted different procedures to calculate the P-values from the observed and expected results under the assumption of randomness [12,13,14,15]. The Test Suite has been coded by us and used to study the randomness features of AES with different S-Boxes.

4. Results and Discussions

Rijndael generated the AES S-Box using the irreducible polynomial {11B} and additive constant {63}. From other valid polynomials and constants extracted, we selected 8 different S-Boxes generated by arbitrarily selected 8 8-bit additive constants (0A, 31, 4A, 74, 9D, CA, D5 and F0) from the set of 36 polynomials, as described above, for the modulus {11D}. It is to be noted that quite a large number of different unknown S-Boxes can be generated by this way, which creates a tweak in AES to increase its security. As the S-Boxes are all unknown, they thus prevent / harden the linear and differential cryptanalysis [10], [12,13,14]. Moreover, the modulus and the additive constant, which may be taken as user-inputs, work as additional keys of AES [15].

In Appendix A, the 8 S-Boxes generated by the irreducible polynomial {11D} are displayed. Distribution of Proportion-of-Passing of P-values (POP) generated by the 15 NIST Tests for these 8 S-Boxes are displayed in Appendix B. POP values compared to the expected values for these 8 S-Boxes are displayed in Appendix C. Histograms on distribution of POP values of two tests (5 & 10), and Scattered Graphs on POP Status of the 15 tests for the 8 S-Boxes are displayed in Appendix D(1) and D(2) respectively.

After analyzing the outputs of the 8 S-Boxes generated and the output of the standard AES S-Box, we compared them to find if a particular S-Box is more secured than the others. In Table-1, the POP values of the NIST tests for these 9 arbitrarily selected S-Boxes are displayed and compared. The best values of a particular test for each S-Box are shaded (in rows) and then the numbers of shaded cells for each S-box are counted (in columns). The highest count (here 4) gives the best result for that S-Box, which shows that this particular S-Box (here {11D_31}) has higher POPs than the others, at least for this particular data-set. It has been observed that the result shown by it is even better than the standard polynomial {63} for modulus 11B. Finally, it has been observed that a number of modulus and additive constant polynomials can be used to generate secured unknown AES S-Boxes, which may give even better randomization in ciphertexts and thus can also prevent linear and differential cryptanalysis.

5. Conclusion

Most of the AES S-Boxes generated, are found to stand in the same or even in the better merit list comparing to the standard S-Box. It also seems that security in AES will be enhanced with additional keys, which are actually the unknown moduli and additive constant polynomials as user-inputs. The user can choose and generate any S-Box according to his / her own choice (i.e., unknown S-Boxes) from a large set of options, preventing linear and differential cryptanalysis. In case of suspicion of a trapdoor in the ciphertext, an S-Box might be replaced by another one by the user. Further study on this is required to find better opportunities to generate secured AES S-Boxes.

References

[1] Foruzan BA, Cryptography and Network Security, Tata McGraw-Hill, New Delhi, Spl. Indian Edition (2007).

[2] Stallings W, Cryptography and Network Security, Pearson Prentice Hall, New Delhi, 6th Impression, (2008).

[3] Stinson DR, Cryptography – Theory and Practice (2002) Dept. of Combinatorics & Optimization, Univ. of Waterloo, Ontario, Canada.

[4] Church R, Tables of irreducible polynomials for the first four prime moduli, The Annals of Maths., 2nd Series, vol. 36, no. 1, 198-209, Jan (1935) http://www .jstor.org/stable/1968675.

[5] Daemen J and Rijmen V, AES Proposal: Rijndael, Version 2, Submitted to NIST, March (1999) http://csrc.nist.gov/encrytion/aes.

[6] Federal Information Processing Standards Publication (FIPS), Announcing the Advanced Encryption Standard (AES) (2001) http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[7] FIPS, PUB 197: the Official AES Standard, 2001-11-26, Retrieved (2010) http://csrc. nist.gov/publications/fips/fips197/fips-197.pdf.

[8] National Institute of Standards & Technology (NIST), Technology Administration, U.S. Dept. of Commerce, A Statistical Test Suite for RNGs and PRNGs for cryptographic applications, (2010) http://csrc. nist.gov/publications/nistpubs800/22rec1SP800-22red1.pdf.

[9] Kim SJ, Umeno K, Hasegawa A, Corrections of the NIST Statistical Test Suite (2004) Comm. Research Lab. Inc., Tokyo, Japan.

[10] Kazilauskas K and Kazilauskas J, Key-dependent S-Box generation in AES block cipher system, Informatica (2009) Inst. of Maths & Informatics, Vilnius, Lithuania

[11] Zaman JKMSU and Ghosh R, A review study of NIST Statistical Test Suite: Development of an indigenous computer package, Institute of Radio Physics & Electronics, University of Calcutta, Kolkata, India, 2011.

[12] Hosseinkhani R et. al., Using cipher key to generate dynamic S-Box in AES cipher system, Islamic Azad Univ. Tehran, Iran, Int. J. Comp Science & Security (IJCSS), vol. 6 (2012).

[13] Paul R, Saha S, Zaman JKMSU, Das S, Chakrabarti A and Ghosh R, A simple 1-byte 1-clock RC4 hardware design and its implementation in FPGA coprocessor for secured Ethernet communication, Proc. National Workshop on Cryptology, VIT University & CRSI, Vellore, India, Aug 6-8, 2012.

[14] Jingmei L, et. al.,One AES S-box to increase complexity and its cryptanalysis, J. Sys. Engg & Elec, Elsevier, vol. 18, no. 2, 427-433 (2007) Xidian University, China.

[15] Das S, Generation of AES-like 8-bit random S-Box and comparative study on randomness of corresponding ciphertexts with other 8-bit AES S-Boxes, Int. Conf. on Advanced Computing, N/w & Informatics (ICACNI-13), CIT, Raipur, India, June, 2013, ISSN: 1867-5662.

Table 1. Comparison of POP values generated by the 15 NIST tests for the selected 8 AES encryption S-Boxes

Tests↓	11B_63	11D_0A	11D _31	11D _4A	11D _74	11D _9D	11D _CA	11D _D5	11D _F0
1	0.960000	0.976667	0.980000	0.976667	0.980000	0.970000	0.966667	0.976667	0.966667
2	0.993333	0.983333	0.976667	0.976667	0.986667	0.983333	0.986667	0.986667	0.970000
3	0.973333	0.953333	0.953333	0.966667	0.973333	0.970000	0.970000	0.976667	0.963333
4	0.943333	0.953333	0.953333	0.956667	0.940000	0.963333	0.943333	0.943333	0.980000
5	0.993333	0.986667	0.976667	0.983333	0.990000	0.980000	0.983333	0.986667	0.983333
6	0.983333	0.990000	0.986667	0.990000	0.980000	0.983333	0.996667	0.983333	0.986667
7	0.976667	0.976667	0.996667	0.986667	0.990000	0.986667	0.990000	0.983333	0.960000
8	0.976667	0.976667	0.983333	0.976667	0.960000	0.976667	0.980000	0.973333	0.970000
9	0.990000	0.993333	0.986667	0.993333	0.990000	0.980000	0.970000	0.986667	0.983333
10	0.986667	0.990000	1.000000	0.980000	0.986667	0.993333	0.993333	0.996667	0.996667

11	0.956667	0.958333	0.941667	0.950000	0.946667	0.960000	0.953333	0.978333	0.956667
12	0.950000	0.946667	0.936667	0.946667	0.943333	0.963333	0.936667	0.970000	0.953333
13	0.986667	0.996667	0.985000	0.988333	0.995000	0.993333	0.985000	0.995000	0.980000
14	0.987083	0.981250	0.987083	0.981250	0.987083	0.979167	0.988333	0.983333	0.983750
15	0.988519	0.980185	0.989815	0.986481	0.991852	0.989444	0.991852	0.989444	0.987963
Count	**2**	**2**	**4**	**1**	**2**	**0**	**3**	**3**	**1**

Appendix A. Generated S-Boxes

Table A1(a). S-Box by Modulus {11D} and Additive {0A}

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

Table A1(b). S-Box by Modulus {11D} and Additive {31}

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

Table A1(c). S-Box by Modulus {11D} and Additive {4A}

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

Table A1(d). S-Box by Modulus {11D} and Additive {74}

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

Table A1(e). S-Box by Modulus {11D} and Additive {9D}

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

Table A1(f). S-Box by Modulus {11D} and Additive {CA}

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

Table A1(g). S-Box by Modulus {11D} and Additive {D5}

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

Table A1(f). S-Box by Modulus {11D} and Additive {F0}

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

Fig. 3(a)&3(b). Results of Test 5 & 10 for Additive {4A}

Fig. 4(a)&4(b). Results of Test 5 & 10 for Additive {74}

Appendix D(1). Histograms on POP Distribution

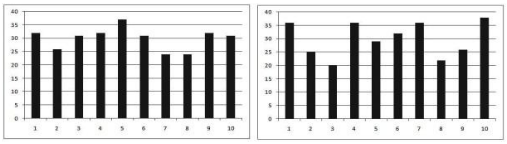

Fig. 1(a)&1(b). Results of Test 5 & 10 for Additive {0A}

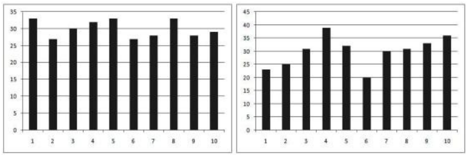

Fig. 2(a)&2(b). Results of Test 5 & 10 for Additive {31}

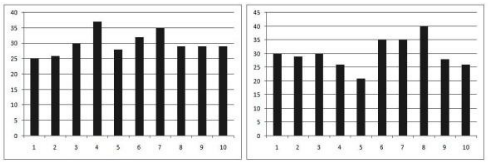

Fig. 3(a)&3(b). Results of Test 5 & 10 for Additive {4A}

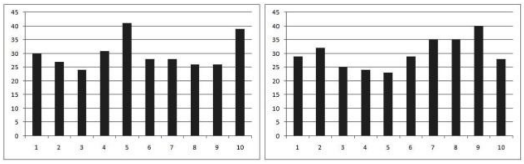

Fig. 4(a)&4(b). Results of Test 5 & 10 for Additive {74}