Generation of AES S-Boxes with Various Additive Polynomials and Testing their Randomization

S. Das, J.K.M.S. Uz Zaman, R. Ghosh

Inst. of Radio Physics & Electronics, University of Calcutta,
92 APC Road, Kolkata – 700 009, India
aami.suman@gmail.com

***Abstract*— In AES, the standard S-Box is usually generated by using a particular irreducible polynomial {11B} in GF(2^8), with a particular additive constant {63}. In this paper, it has been shown that, by maintaining the criteria defined by Rijndael, other constants can also be used with the same modulus polynomial to generate different unknown S-Boxes. 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 additive constants are also able to generate equally or better random ciphertexts. Moreover, the additive constant acts as a secondary key, thus increasing the key-space.**

Keywords-AES S-Box, Random S-Box, NIST Test Suite, AES Additive Constant, AES Secondary Key.

I. 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 Federal Information Processing Standards (FIPS). In AES encryption, to introduce non-linearity, an 8-bit S-Box has been generated using modular arithmetic in GF(2^8). Based on this forward S-Box, the inverse S-Box is built for decryption [1]-[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 byte {63} in GF(2). Though in the original proposal of AES, Rijndael used this particular additive constant, it has been found that other constants can also be used as the additive, making the generation of the S-Box more dynamic [5]-[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.

II. 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 an irreducible polynomial in GF(2^8) as the modulus – the inverse of zero is mapped to itself. The multiplicative inverses are then transformed into the final substitutions as shown in eq.(1) – here the operations are in GF(2):

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

for $0 \le i < 8$, 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]–[7].

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

This conventional AES 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 [Table A2(B)]. Rows and columns of an AES S-Box are determined by the most and the least significant nibbles of each byte respectively.

Rijndael proposed to choose 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 the valid 8-bit constants in the range 0-255 (00000000 to 11111111, i.e., {00}-{FF}) that can be used as an additive constant (c) in eq. (1) and (2). A list of them is as follows (values are given hexadecimal notation):

05, 07, 08, 15, 1D, 20, 30, 37, 38, 3B, 3D, 49,
52, 56, 5D, 63, 76, 89, 9C, A2, A9, AD, B6,
C2, C4, C7, C8, CF, DF, E2, EA, F7, F8, FA.

We have generated all the S-Boxes using the above additive constants and arbitrarily selected 8 of them from the set for AES encryption and encrypted a text file 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].

ISBN: 978-81-923777-9-7

III. 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]–[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*: If frequency of 1's in an M-bit block is approximately M/2.
3) *Runs Test*: No. 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 no. 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 $m + 1$).
13) *Cumulative Sums Test*: Finds if 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.
14) *Random Excursions Test*: Finds if no. of visits to a state within a cycle deviates from expected value, calculates the no. of cycles having exactly K visits in a cumulative sum random walk.
15) *Random Excursions Variant Test*: Deviations from the expected visits to various states in the random walk, calculates the no. 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]–[15]. The Test Suite has been coded by us and used to study the randomness features of AES with different S-Boxes.

IV. RESULTS AND DISCUSSIONS

Rijndael generated the AES S-Box using the additive constant polynomial {63}. From the remaining valid 8-bit constants extracted, we selected 8 different S-Boxes generated by arbitrarily selected 8 additive constants from the set of 34 polynomials, as described above. 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], [14]. Moreover, the additive constant, which may be taken as a user-input, works as a secondary key of AES [15].

POPs generated by 4 of these 8 S-Boxes for the 15 tests, compared to the expected values, are displayed in Appendix-I. The 8 S-Boxes generated are displayed in Appendix-II. Distribution of Proportion-of-Passing of P-values (POP) generated by the 15 NIST Tests for these 8 S-Boxes are displayed in Appendix-III. Histograms on distribution of POP values of two tests (5 & 10), and Scattered Graphs on the POPs of the 15 tests are displayed in Appendix-IV(a) and IV(b) respectively.

After analyzing the outputs of the 8 S-Boxes, we compared them to find if a particular S-Box is more secured than the others. In Table-I, the POP values of the NIST tests for these 8 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 6) gives the best result for a particular S-Box, which shows that this particular S-Box (here {49}) has a better POP than the others, at least for this particular data-set. It has been observed that the results shown by the additive constant {49} is even better than the standard polynomial {63}.

Finally, it has been observed that a number of additive constant polynomials can be used to generate a secured unknown AES S-Box, which may give even better randomization in ciphertexts and also prevents linear and differential cryptanalysis.

V. CONCLUSION

All 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 a secondary key, which is actually the unknown additive constant polynomial as a user-input The user can choose and generate any S-Box according to his / her own choice of additive constants (i.e., unknown S-Boxes) from a large set of options, preventing linear and differential cryptanalysis. In the 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.

ISBN: 978-81-923777-9-7

REFERENCES

[1] B. A. Foruzan, *Cryptography and Network Security*, Tata McGraw-Hill, New Delhi, Spl. Indian Edition, 2007.

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

[3] D. R. Stinson, *Cryptography – Theory and Practice*, 2002, Dept. of Combinatorics & Optimization, Univ. of Waterloo, Ontario, Canada.

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

[5] J. Daemen and V. Rijmen, *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 2010-04-29, 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*, http://csrc. nist.gov/publications/nistpubs800/22rec1SP800-22red1.pdf.

[9] S. J. Kim, K. Umeno, A. Hasegawa, *Corrections of the NIST Statistical Test Suite for randomness*, Comm. Research Lab. Inc., Tokyo, Japan.

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

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

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

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

[15] S. Das, *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 Adv. Comp., N/w & Info. (ICACNI), June, 2013, Central Institute of Technology, Raipur, India. ISSN: 1867-5662

TABLE I. COMPARISON OF POP VALUES GENERATED BY THE 15 NIST TESTS FOR THE SELECTED 8 AES ENCRYPTION S-BOXES

Tests↓	**{05}**	**{49}**	**{63}**	**{89}**	**{B6}**	**{C4}**	**{CF}**	**{F7}**
1	0.973333	0.980000	0.960000	0.956667	0.963333	0.966667	0.976667	0.956667
2	0.993333	0.993333	0.993333	0.973333	0.980000	0.990000	0.966667	0.993333
3	0.976667	0.980000	0.973333	0.976667	0.976667	0.973333	0.976667	0.953333
4	0.976667	0.976667	0.943333	0.970000	0.953333	0.970000	0.956667	0.963333
5	0.986667	0.980000	0.993333	0.990000	0.996667	0.986667	0.993333	0.990000
6	0.990000	1.000000	0.983333	0.990000	0.990000	0.983333	0.993333	0.983333
7	0.983333	0.976667	0.976667	0.966667	0.980000	0.970000	0.983333	0.986667
8	0.960000	0.980000	0.976667	0.980000	0.976667	0.973333	0.976667	0.976667
9	0.983333	0.983333	0.990000	0.983333	0.983333	1.000000	0.980000	0.973333
10	0.986667	0.986667	0.986667	0.993333	0.983333	0.993333	0.986667	0.996667
11	0.980000	0.946667	0.956667	0.956667	0.950000	0.955000	0.953333	0.953333
12	0.976667	0.940000	0.950000	0.950000	0.936667	0.946667	0.946667	0.950000
13	0.988333	0.993333	0.986667	0.993333	0.995000	0.995000	0.993333	0.993333
14	0.987500	0.986667	0.987083	0.984583	0.986250	0.986667	0.988333	0.986250
15	0.987407	0.986296	0.988519	0.993148	0.986111	0.987593	0.987778	0.982593
	4	**6**	**1**	**2**	**2**	**2**	**1**	**3**

APPENDIX–I. POP STATUS FOR VARIOUS S-BOXES

TABLE A1(A)
POPS FOR ADDITIVE CONSTANT {05}

Test	Expected POP	Observed POP	Status
1	0.972766	0.973333	Successful
2	0.972766	0.993333	Successful
3	0.972766	0.976667	Successful
4	0.972766	0.976667	Successful
5	0.972766	0.986667	Successful
6	0.972766	0.990000	Successful
7	0.972766	0.983333	Successful
8	0.972766	0.960000	Unsuccessful
9	0.972766	0.983333	Successful
10	0.972766	0.986667	Successful
11	0.977814	0.980000	Successful
12	0.972766	0.976667	Successful
13	0.977814	0.988333	Successful
14	0.983907	0.987500	Successful
15	0.985938	0.987407	Successful

TABLE A1(B)
POPS FOR ADDITIVE CONSTANT {49}

Test	Expected POP	Observed POP	Status
1	0.972766	0.980000	Successful
2	0.972766	0.993333	Successful
3	0.972766	0.980000	Successful
4	0.972766	0.976667	Successful
5	0.972766	0.980000	Successful
6	0.972766	1.000000	Successful
7	0.972766	0.976667	Successful
8	0.972766	0.980000	Successful
9	0.972766	0.983333	Successful
10	0.972766	0.986667	Successful
11	0.977814	0.946667	Unsuccessful
12	0.972766	0.940000	Unsuccessful
13	0.977814	0.993333	Successful
14	0.983907	0.986667	Successful
15	0.985938	0.986296	Successful

TABLE A1(C)
POPS FOR ADDITIVE CONSTANT {63}

Test	Expected POP	Observed POP	Status
1	0.972766	0.960000	Unsuccessful
2	0.972766	0.993333	Successful
3	0.972766	0.973333	Successful
4	0.972766	0.943333	Unsuccessful
5	0.972766	0.993333	Successful
6	0.972766	0.983333	Successful
7	0.972766	0.976667	Successful
8	0.972766	0.976667	Successful
9	0.972766	0.990000	Successful
10	0.972766	0.986667	Successful
11	0.977814	0.956667	Unsuccessful
12	0.972766	0.950000	Unsuccessful
13	0.977814	0.986667	Successful
14	0.983907	0.987083	Successful
15	0.985938	0.988519	Successful

TABLE A1(D)
POPS FOR ADDITIVE CONSTANT {89}

Test	Expected POP	Observed POP	Status
1	0.972766	0.956667	Unsuccessful
2	0.972766	0.973333	Successful
3	0.972766	0.976667	Successful
4	0.972766	0.970000	Unsuccessful
5	0.972766	0.990000	Successful
6	0.972766	0.990000	Successful
7	0.972766	0.966667	Successful
8	0.972766	0.980000	Successful
9	0.972766	0.983333	Successful
10	0.972766	0.993333	Successful
11	0.977814	0.956667	Unsuccessful
12	0.972766	0.950000	Unsuccessful
13	0.977814	0.993333	Successful
14	0.983907	0.984583	Successful
15	0.985938	0.993148	Successful

ISBN: 978-81-923777-9-7

Appendix–II. Various AES S-Boxes Generated

Table A2(a)
S-Box Generated by the Additive Constant {05}

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

Table A2(b)
S-Box Generated by the Additive Constant {63}

	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
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

Table A2(c)
S-Box Generated by the Additive Constant {49}

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

Table A2(d)
S-Box Generated by the Additive Constant {89}

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

Table A2(e)
S-Box generated by Additive Constant {B6}

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

Table A2(f)
S-Box generated by Additive Constant {C4}

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

Table A2(g)
S-Box Generated by the Additive Constant {F7}

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

Table A2(h)
S-Box Generated by the Additive Constant {CF}

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

ISBN: 978-81-923777-9-7

APPENDIX–III. POP DISTRIBUTIONS FOR TEST NO. 5

TABLE A3(A) *

POP DISTRIBUTION BY ADDITIVE CONSTANT {05}

	0	1	2	3	4	5	6	7	8	9	10
1	8	34	37	29	23	36	24	28	19	35	27
2	2	39	33	28	23	24	29	31	26	26	39
3	7	41	33	25	29	33	26	23	30	24	29
4	7	46	40	29	28	31	15	31	32	18	23
5	4	39	36	25	28	19	36	27	23	31	32
6	3	28	30	24	24	36	34	31	39	24	27
7	5	37	31	44	27	24	32	14	25	35	26
8	12	46	34	41	31	34	20	23	20	20	19
9	5	31	34	29	31	21	29	34	29	25	32
10	4	28	34	30	33	26	28	38	33	20	26
11	12	96	82	70	69	56	50	45	44	43	33
12	7	51	38	34	35	34	25	23	21	19	13
13	7	65	62	46	66	54	59	60	60	67	54
14	30	241	233	237	268	244	226	219	234	222	246
15	68	481	488	517	583	544	528	531	562	556	542

TABLE A3(B)

POP DISTRIBUTION BY ADDITIVE CONSTANT {63}

	0	1	2	3	4	5	6	7	8	9	10
1	12	45	34	36	17	32	26	33	16	30	19
2	2	30	30	34	34	35	25	18	27	31	34
3	8	46	49	26	26	29	24	20	26	25	21
4	17	55	36	43	24	23	24	23	24	16	15
5	2	34	40	30	30	26	30	30	25	28	25
6	5	31	29	31	21	29	23	25	41	30	35
7	7	31	43	31	28	26	27	20	32	37	18
8	7	41	35	42	34	28	29	17	18	24	25
9	3	35	35	28	37	28	27	21	28	30	28
10	4	32	25	25	24	38	33	30	22	34	33
11	26	94	77	64	65	69	43	42	43	46	31
12	15	57	43	32	30	33	21	19	23	15	12
13	8	50	50	46	68	60	60	69	71	69	49
14	31	230	240	231	244	231	238	234	255	254	212
15	62	435	515	570	564	533	574	484	556	546	561

TABLE A3(C)

POP DISTRIBUTION BY ADDITIVE CONSTANT {49}

	0	1	2	3	4	5	6	7	8	9	10
1	6	42	38	33	31	25	23	28	29	17	28
2	2	35	26	44	16	26	24	24	28	36	39
3	6	37	37	29	33	30	21	35	19	20	33
4	7	39	37	34	35	24	30	25	21	33	15
5	6	23	43	29	41	29	35	23	20	23	28
6	0	27	35	41	26	27	27	29	28	31	29
7	7	41	41	22	35	27	23	27	27	28	22
8	6	45	35	44	27	31	24	28	20	18	22
9	5	39	31	31	24	33	30	32	28	27	20
10	4	30	25	27	37	30	32	27	25	32	31
11	32	97	89	61	51	38	41	58	47	47	39
12	18	47	48	42	23	17	17	32	17	19	20
13	4	70	69	67	55	60	63	55	56	49	52
14	32	192	235	226	236	264	257	226	254	241	237
15	74	389	516	561	545	541	559	549	560	566	540

TABLE A3(D)

POP DISTRIBUTION BY ADDITIVE CONSTANT {89}

	0	1	2	3	4	5	6	7	8	9	10
1	13	52	37	32	22	24	27	17	22	24	30
2	8	29	30	30	30	21	31	22	28	32	39
3	7	43	43	29	34	16	31	14	29	32	22
4	9	51	31	38	29	23	26	27	25	27	14
5	3	27	28	32	33	24	22	33	29	36	33
6	3	28	35	34	25	27	24	38	38	27	21
7	10	46	31	32	28	28	30	30	22	25	18
8	6	42	43	36	29	32	28	16	26	21	21
9	5	26	39	31	26	35	25	26	32	22	33
10	2	20	28	32	36	24	32	37	33	29	27
11	26	130	77	64	62	46	42	42	39	38	34
12	15	71	40	30	36	25	13	21	16	23	10
13	4	50	77	63	49	49	56	66	64	54	68
14	37	202	225	223	247	242	250	253	254	251	216
15	37	417	538	557	548	540	553	553	559	545	553

TABLE A3(E)

POP DISTRIBUTION BY ADDITIVE CONSTANT {B6}

	0	1	2	3	4	5	6	7	8	9	10
1	11	42	36	34	34	17	24	28	23	28	23
2	6	28	39	31	36	26	26	22	19	32	35
3	7	36	42	31	27	31	15	36	29	30	16
4	14	41	39	38	33	32	23	22	15	21	22
5	1	35	30	27	33	30	30	28	30	27	29
6	3	23	30	35	21	47	25	34	32	24	26
7	6	44	49	24	28	24	32	26	19	25	23
8	7	43	34	33	35	31	36	25	20	18	18
9	5	35	33	20	32	32	23	23	25	37	35
10	5	35	23	28	26	33	32	32	31	26	29
11	30	92	89	66	57	53	49	39	43	42	40
12	19	48	41	36	26	36	25	15	17	17	20
13	3	51	53	68	58	65	55	57	56	65	69
14	33	217	240	239	233	259	246	227	227	242	237
15	75	499	559	566	540	505	508	532	524	563	529

TABLE A3(F)

POP DISTRIBUTION BY ADDITIVE CONSTANT {C4}

	0	1	2	3	4	5	6	7	8	9	10
1	10	34	36	29	29	28	28	30	29	22	25
2	3	30	29	27	27	31	21	35	33	33	31
3	8	38	39	29	24	31	17	28	34	24	28
4	9	42	45	38	32	26	32	21	20	17	18
5	4	32	28	29	26	42	31	18	31	28	31
6	5	24	29	30	24	32	25	30	46	26	29
7	9	33	42	21	30	28	33	25	28	28	23
8	8	55	36	25	21	33	28	25	28	28	13
9	0	21	32	30	30	41	25	26	31	26	38
10	2	28	31	24	40	36	22	24	40	28	25
11	27	102	61	50	47	53	65	49	51	52	43
12	16	54	33	27	23	21	37	23	20	31	15
13	3	50	67	68	72	60	51	62	64	47	56
14	32	220	230	240	236	226	241	258	218	243	256
15	67	448	543	625	546	558	536	507	518	513	539

TABLE A3(G)

POP DISTRIBUTION BY ADDITIVE CONSTANT {F7}

	0	1	2	3	4	5	6	7	8	9	10
1	13	37	37	32	20	42	23	26	24	18	28
2	2	29	30	35	29	24	27	24	30	34	36
3	14	41	40	36	23	19	28	24	26	29	20
4	11	56	47	38	29	29	16	17	19	19	19
5	3	34	28	41	32	24	34	27	27	31	19
6	5	27	26	28	22	28	22	29	50	32	31
7	4	34	40	37	32	35	25	25	23	21	24
8	7	44	39	37	31	30	24	27	18	23	20
9	8	29	31	29	31	37	35	19	23	34	24
10	1	32	39	30	24	33	35	36	18	27	25
11	28	98	88	53	64	43	52	47	41	44	42
12	15	58	52	26	28	24	23	22	19	15	18
13	4	56	66	56	49	56	69	67	63	58	56
14	33	227	250	221	236	241	245	246	220	231	250
15	94	484	573	547	522	526	537	509	538	559	511

TABLE A3(G)

POP DISTRIBUTION BY ADDITIVE CONSTANT {CF}

	0	1	2	3	4	5	6	7	8	9	10
1	7	60	30	28	26	23	26	20	21	26	33
2	10	25	38	20	24	34	34	24	26	25	40
3	7	44	35	35	29	28	24	30	29	22	17
4	13	52	35	33	32	26	31	13	17	25	23
5	2	33	29	39	27	24	28	27	22	35	34
6	2	30	30	31	23	33	20	39	35	28	29
7	5	41	32	30	36	30	23	26	27	23	27
8	7	45	47	27	26	32	19	23	25	30	19
9	6	38	19	32	26	36	29	27	32	26	29
10	4	20	37	34	30	25	28	31	30	28	33
11	28	124	74	67	62	50	60	42	36	35	22
12	16	68	39	30	37	23	31	15	13	17	11
13	4	49	73	49	64	69	61	50	65	53	63
14	28	199	255	222	255	242	252	254	256	188	249
15	66	474	541	548	546	551	569	523	533	537	512

* Horizontal Ranges for Tables: 1: .0-.1, 2: >.1-.2, 3: >.2-.3, …., 10: >.9-1

ISBN: 978-81-923777-9-7

APPENDIX–IV(A). HISTOGRAMS FOR POP DISTRIBUTION

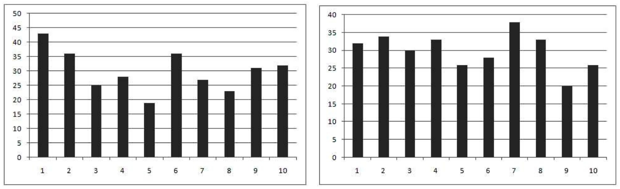

Figure 1(a)&1(b). Results of Test 5 & 10 for Additive Constant {05}

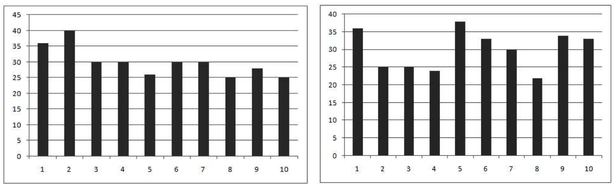

Figure 2(a)&2(b). Results of Test 5 & 10 for Additive Constant {63}

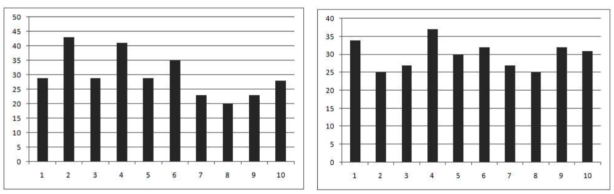

Figure 3(a)&3(b). Results of Test 5 & 10 for Additive Constant {49}

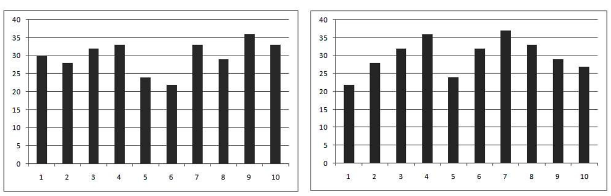

Figure 4(a)&4(b). Results of Test 5 & 10 for Additive Constant {89}

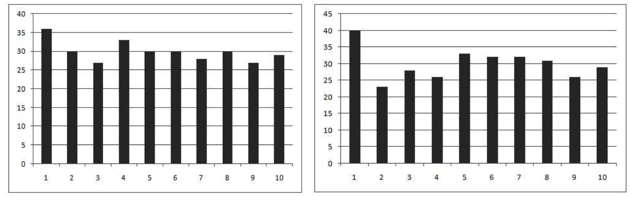

Figure 5(a)&5(b). Results of Test 5 & 10 for Additive Constant {B6}

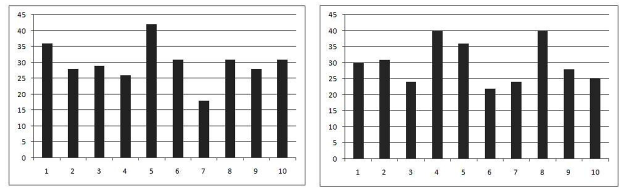

Figure 6(a)&6(b). Results of Test 5 & 10 for Additive Constant {C4}

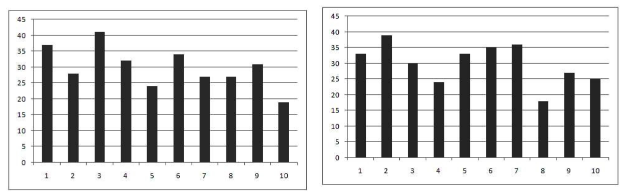

Figure 7(a)&7(b). Results of Test 5 & 10 for Additive Constant {F7}

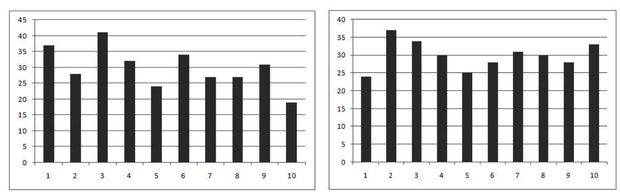

Figure 8(a)&8(b). Results of Test 5 & 10 for Additive Constant {CF}

APPENDIX – IV(B). P-VALUE PLOTS FOR 15 NIST TESTS

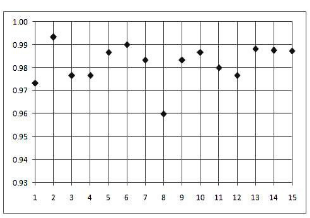

Figure 9. Additive Const. {05}

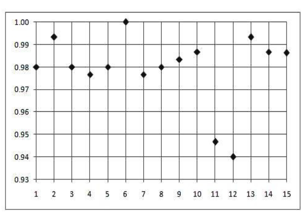

Figure 10. Additive Const. {49}

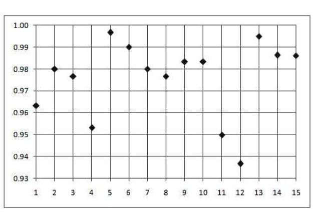

Figure 11. Additive Const. {B6}

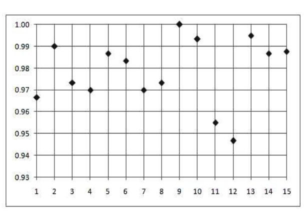

Figure 12. Additive Const. {C4}

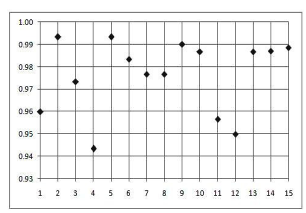

Figure 13. Additive Const. {63}

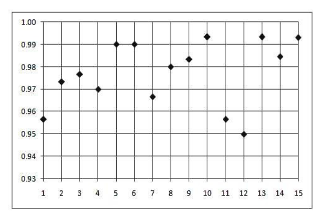

Figure 14. Additive Const. {89}

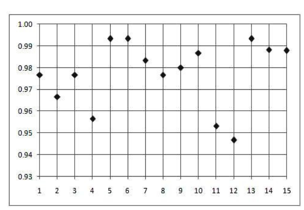

Figure 15. Additive Const. {CF}

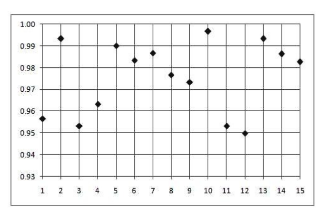

Figure 16. Additive Const. {F7}

ISBN: 978-81-923777-9-7