Bent Boolean functions: A better procedure to generate non-crypto 4-bit S-boxes.

Sankhanil Dey[1] and Ranjan Ghosh[2],
Department of Radio Physics and Electronics, University of Calcutta,
92 A P C Road, Kolkata-700009[1,3].

Abstract: crypto 4-bit substitution boxes or crypto 4-bit S-boxes are used in block ciphers for nonlinear substitution very frequently. If the 16 elements of a 4-bit S-box are unique, distinct and vary between 0 and f in hex then the said 4-bit S-box is called as a crypto 4-bit S-box. There are 16! crypto 4-bit S-boxes available in crypto literature. Other than crypto 4-bit S-boxes there are another type of 4-bit S-boxes exist. In such 4-bit S-boxes 16 elements of the 4-bit S-box are not unique and distinct i.e. at least one element must repeat more than one time. They are called as non-crypto 4-bit S-boxes. There are 16^{16}-16! Numbers of non-crypto 4-bit S-boxes can be found in crypto-literature. The non-crypto 4-bit S-boxes can be generated from 4-bit Boolean Functions (BFs) in the same manner as crypto 4-bit S-boxes are generated in [1]. But to generate crypto 4-bit S-boxes the security of the generated 4-bit S-boxes is sacrificed into some extend. Since 12870 4-bit balanced BFs are responsible for 16! crypto 4-bit S-boxes and the nonlinearity of the balanced 4-bit BFs are at most 4. So the 4-bit BFs with highest nonlinearity 6 are left abandoned. These 4-bit BFs are called as 4-bit Bent BFs. Here in this paper we generate non-crypto 4-bit S-boxes from 4-bit Bent BFs. The generated non-crypto 4-bit S-boxes are analyzed with the existing cryptanalysis techniques to prove them much secure 4-bit S-boxes from crypto angle.

1. **Introduction and Scope:** 4-bit S-boxes are made of 16 elements. The hex values of 16 elements of a 4-bit S-box are may or may not be unique and distinct. If the 16 elements have 16 unique hex values varies from 0 to F in hex then the 4-bit S-box is termed as crypto 4-bit S-box [2]. Left alone 4-bit S-boxes are non-crypto 4-bit S-boxes. In non-crypto 4-bit S-boxes 16 elements must not have 16 unique hex values and the hex values must be within 0 to F in hex. For a brief example a crypto 4-bit S-box is given in row 1 of table.1.1 and a non-crypto 4-bit S-box is given in row 2 of table.1.1. Here Index 0 is termed as the position of Most Significant Element (MSE) and Index F is termed as position of Least Significant Element (LSE) respectively.

Row	**Index**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
1	**Crypto**	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	**Non-crypto**	0	0	1	1	2	2	3	4	5	6	7	8	9	A	A	B

Table.1.1: A brief example of a crypto 4-bit S-box (identity 4-bit S-box) and a non-crypto 4-bit S-box.

Each of 16 elements from MSE to LSE of a crypto 4-bit S-box are converted into 16-bit long binary numbers. The first MSBs (as given in table.1.2) of each of 16 elements from MSE to LSE constitutes 4th output BF or 4th OPBF. In the same manner 2nd bits from MSB, 3rd bit from MSB and LSBs constitute 3rd output BF or 3rd OPBF, 2nd output BF or 2nd OPBF and 1st output BF or 1st OPBF respectively [3][4]. The non-crypto 4-bit S-boxes are decomposed into four OPBFs in the same manner. The four OPBFs of the crypto 4-bit S-box are given in table.1.1 and are shown in row 2, 3, 4, 5 of table.1.2 with the four OPBFs of the non-crypto 4-bit S-box are given in table.1.1 and are shown in row 8, 9, 10 and 11 of table.1.2 respectively. The table.1.2 is given as follows,

Row	Index	MSB	Crypto 4-bit S-box															
			0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
1	**Crypto**		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	**4th OPBF**	Bal	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
3	**3rd OPBF**	Bal	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
4	**2nd OPBF**	Bal	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
5	**1st OPBF**	Bal	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
6		LSB	**Non crypto 4-bit S-box**															
7	**Non-crypto**	MSB	0	0	1	1	2	2	3	4	5	6	7	8	9	A	A	B
8	**4th OPBF**	Unbal	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1
9	**3rd OPBF**	Unbal	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0
10	**2nd OPBF**	Unbal	0	0	0	0	1	1	1	0	0	1	1	0	0	1	1	1
11	**1st OPBF**	Unbal	0	0	1	1	0	0	1	0	1	0	1	0	1	0	0	1
12		LSB	**Table.1.2**: crypto and non-crypto 4-bit S-box to 4-bit BFs															

In this example as well as in related relevant crypto literature it is found that the four OPBFs of a crypto 4-bit S-box must be balanced but the four OPBFs of a non-crypto 4-bit S-box may or may not be balanced [3][4]. So the maximum nonlinearity of any OPBF of a crypto 4-bit S-box is at most 4 [2]. So the security of a crypto 4-bit S-box has certain limitations far below maximum. But the non-crypto 4-bit S-boxes can be generated from unbalanced OPBFs. So the maximum nonlinearity of any OPBF of a non-crypto 4-bit S-box is at most 6 .i.e. the maximum value of the maximum nonlinearity. The BFs with maximum nonlinearity 6 are called as 4-bit Bent Boolean functions or 4-bit Bent BFs. The non-crypto S-boxes generated from Bent BFs must have good security.

In this paper 4-bit Bent Boolean function is defined with proper example in section 2. The generation of non-crypto 4-bit S-boxes from 4-bit Bent functions is explained with example in section 3. And the generated non-crypto 4-bit S-boxes are analyzed with latest cryptanalysis techniques to show the result in section 4. The results and the utility of non-crypto S-boxes in encryption and decryption algorithms are also established in section 5. Section 6 is dedicated to the conclusion of this research article.

2. 4-bit Bent Boolean functions: The maximum nonlinearity described in [2] is one of the key features to select 4-bit BFs for generation of 4-bit S-boxes. In Lucifer [5][6] and DES [7][8] crypto 4-bit S-boxes are used for nonlinear substitution and these crypto 4-bit S-boxes must be composed of balanced [2] 4-bit BFs. So the maximum nonlinearity of the 4-bit BFs used in generation of crypto 4-bit S-boxes are at most 4. So the security of the 4-bit S-boxes in generated crypto 4-bit S-boxes by balanced 4-bit BFs is neglected. Now it can be seen from file entitled "4-bit Bent BFs" is that the maximum nonlinearity of 4-bit BFs is 6. There are 448 nonlinear [8] and their complement 448 non-affine [2] 4-bit BFs exist with nonlinearity 6. These 996 4-bit BFs are termed as 4-bit Bent BFs. The First Order Strict Avalanche Criterion (FO-SAC) [2], Successive First Order Strict Avalanche Criterion (SFO-SAC) [2], and Multiple Higher Order Strict Avalanche Criterion (MHO-SAC) [2] shows the best results for these 996 4-bit Bent BFs. So these 996 4-bit Bent BFs are the best options to generate 4-bit S-boxes with good security. The only disadvantage is that these 996 4-bit Bent BFs generate only non-crypto S-boxes. Since S-boxes are used for nonlinear substitutions, the arrangement of the algorithm can be able to overcome this disadvantage. So the 4-bit non-crypto S-boxes generated from these 996 4-bit Bent BFs are better ones from the crypto security angle. All these properties of these 996 4-bit Bent BFs are noted in table 2.1 given in appendix which is a part of the c language program generated text file entitled "4-bit Bent BFs" enclosed with this paper as supplementary material. Description of the table and the file is given below.

3.

Description of the table 2.1 or the file "4-bit Bent BFs":

1. Here **Sl.No.** column shows serial numbers of the Bent 4-bit BFs in ascending order of their decimal equivalents and the corresponding complement Bent 4-bit BFs in descending order of their decimal equivalents.

2. Here **BF(Dec)** column shows the decimal equivalents of the Bent 4-bit BFs in ascending order.

3. Here **BF(Binary)** shows the 16 bit long binary output vectors of the Bent 4-bit BFs in ascending order of their decimal equivalents.
4. Here in **10** column **1** shows the numbers of 1s and **0** shows the numbers of 0s in the 16 bit long binary output vectors of the Bent 4-bit BFs.
5. Here **L** column shows that the Bent 4-bit BFs are nonlinear. In this column 1 means Linear Bent 4-bit BFs, 2 means Nonlinear Bent 4-bit BFs, 3 means Affine Bent 4-bit BFs and 4 means Non-Affine Bent 4-bit BFs.
6. Here **CBF(Dec)** column shows the decimal equivalents of the Complement Bent 4-bit BFs in descending order.
7. Here C**BF(Binary)** shows the 16 bit long binary output vectors of the Complement Bent 4-bit BFs in descending order of their decimal equivalents.
8. Here in **10** column **1** shows the numbers of 1s and **0** shows the numbers of 0s in the 16 bit long binary output vectors of the Complement Bent 4-bit BFs.
9. Here **L** column shows that the Complement Bent 4-bit BFs are non-affine. In this column 1 means Linear Complement Bent 4-bit BFs, 2 means Nonlinear Complement Bent 4-bit BFs, 3 means Affine Complement Bent 4-bit BFs and 4 means Non-Affine Complement Bent 4-bit BFs.
10. Here in **Mm** column **M** means maximum hamming distance and **m** means minimum hamming distance among 32 hamming distances of the 16 bit long binary output vectors of the Bent 4-bit BFs to the 16 linear and 16 affine BFs.
11. Here in FO-SAC 8421 column 1 is under 8 means the 4^{th} OPBF satisfies FO-SAC individually. Similarly 1 is under 4 means the 3^{rd} OPBF satisfies FO-SAC individually. Again 1 is under 2 means the 2^{nd} OPBF satisfies FO-SAC individually and 1 is under 1 means the 1st OPBF satisfies FO-SAC individually.
12. Here in column SFO-SAC 3569AB, 1 is under 3 means the 2^{nd} OPBF and 1^{st} OPBF both satisfies FO-SAC individually. Similarly 1 is under 5, 6, 9, A and B means the 3^{rd} OPBF and 1^{st} OPBF, 3^{rd} OPBF and 2^{nd} OPBF, 4^{th} OPBF and 1^{st} OPBF, 4^{th} OPBF and 2^{nd} OPBF and 4^{th} OPBF and 2^{nd} OPBF, both satisfies FO-SAC individually respectively.
1 is under 7, B, D and E means the 3^{rd} OPBF, 2^{nd} OPBF and 1^{st} OPBF, 4^{th} OPBF 2^{nd} OPBF and 1^{st} OPBF, 4^{th} OPBF 3^{rd} OPBF and 1^{st} OPBF and 4^{th} OPBF 3^{rd} OPBF and 2^{nd} OPBF, all satisfies FO-SAC individually respectively.
Here 1 is under F means 4^{th} OPBF, 3^{rd} OPBF, 2^{nd} OPBF and 1^{st} OPBF FO-SAC individually.
13. Here in **SFO-SUM** total numbers of 1s in column SFO-SAC is counted.
14. Here in column MHO-SAC 3569AB, 1 is under 3 means the 2^{nd} OPBF and 1^{st} OPBF both satisfies FO-SAC together. Similarly 1 is under 5, 6, 9, A and B means the 3^{rd} OPBF and 1^{st} OPBF, 3^{rd} OPBF and 2^{nd} OPBF, 4^{th} OPBF and 1^{st} OPBF, 4^{th} OPBF and 2^{nd} OPBF and 4^{th} OPBF and 2^{nd} OPBF, both satisfies FO-SAC together respectively.
1 is under 7, B, D and E means the 3^{rd} OPBF, 2^{nd} OPBF and 1^{st} OPBF, 4^{th} OPBF 2^{nd} OPBF and 1^{st} OPBF, 4^{th} OPBF 3^{rd} OPBF and 1^{st} OPBF and 4^{th} OPBF 3^{rd} OPBF and 2^{nd} OPBF, all satisfies FO-SAC together respectively.
Here 1 is under F means 4^{th} OPBF, 3^{rd} OPBF, 2^{nd} OPBF and 1^{st} OPBF FO-SAC together.
15. Here in **MHO-SUM** total numbers of 1s in column MHO-SAC is counted.

4. Generation of 4-bit non-crypto S-boxes from 996 4-bit Bent BFs: The non-crypto 4-bit S-boxes generated from 4-bit Bent BFs are termed as 4-bit Bent S-boxes. Four Bent BFs are needed to generate a 4-bit Bent S-box. The MSBs of the output vector of four Bent BFs from MSB to LSB constitute a 4-bit binary number. The decimal equivalent (DE) of the 4-bit binary number is the 1^{st} element or MSE of a 4-bit Bent S-box. In the same manner 15 consecutive bits in rest 15 positions of the four 4-bit Bent BFs generate other 15 elements of the S-box.

The 4-bit Bent BF that has complement bits in all positions w.r.t bits in all corresponding positions of a certain 4-bit Bent BF is called as the complement 4-bit Bent BF of the said 4-bit Bent BF. In table.3.1 the 4-bit Bent BF with DE 64681, 64678, 64666 and 64661 are the complement 4-bit Bent BFs of the 4-bit Bent BFs with DE 854, 857, 869 and 874 respectively. So the 2, 4-bit Bent S-boxes generated from 4, 4-bit Bent BFs and their complement 4-bit Bent BFs are complement S-boxes i.e. elements in a certain position of the complement S-box is equal to F- elements in that particular position of the S-box in hex.

Non-crypto S-box																	Complement Non-crypto S-box																
DEs	Output 4-bit Bent BFs																DEs	Complement Output 4-bit Bent BFs															
00854	0	0	0	0	0	0	1	1	0	1	0	1	0	1	1	0	64681	1	1	1	1	1	1	0	0	1	0	1	0	1	0	0	1
00857	0	0	0	0	0	0	1	1	0	1	0	1	1	0	0	1	64678	1	1	1	1	1	1	0	0	1	0	1	0	0	1	1	0
00869	0	0	0	0	0	0	1	1	0	1	1	0	0	1	0	1	64666	1	1	1	1	1	1	0	0	1	0	0	1	1	0	1	0
00874	0	0	0	0	0	0	1	1	0	1	1	0	1	0	1	0	64661	1	1	1	1	1	1	0	0	1	0	0	1	0	1	0	1
S-box	0	0	0	0	0	0	F	F	0	F	3	C	5	A	9	6	S-box	F	F	F	F	F	F	0	0	F	0	C	3	A	5	6	9

Table.3.1: 4-bit Bent S-box generation from 4-bit Bent BFs.

5. Cryptanalysis of 4-bit Bent BFs: Here 3 well known cryptanalysis techniques are used to analyze the 4-bit Bent S-boxes. They are '(Output) Bit Independence Criterion' (BIC) [1] 'Linear Cryptanalysis of 4-bit S-boxes' (LC) [9][10] and 'Differential Cryptanalysis of 4-bit S-boxes' (DC) [9][10]. The numbers of 0s in Linear Approximation Table (LAT) and Difference Distribution Table (DDT) are used to conclude the security. With increase in numbers of 0s in LAT and DDT the security of the non-crypto 4-bit S-boxes increases [9][10]. The results are shown in the table 4.1 in appendix which is a part of the c language program generated text file entitled "Analysis of the non-crypto 4-bit Bent S-boxes" enclosed with this paper as supplementary material. Description of the table and the file is given below.

Description of the table 4.1 or the file "Analysis of the non-crypto 4-bit Bent S-boxes":

1. Here in column Sl. No. the numbers shows the permuted [2] 4-bit Bent S-boxes in ascending order of their hexadecimal equivalents and their corresponding Complement 4-bit Bent S-boxes in descending order of their hexadecimal equivalents.

2. In column **DEs of BFs-crypto S-box SB(DBF1,DBF2,DBF3,DBF4)** DBF1 shows the decimal equivalent of 4th OPBF of the 4-bit Bent S-boxes. Similarly DBF2, DBF3 and DBF4 show decimal equivalents of 3rd OPBF, 2nd OPBF and 1st OPBF of the same.

3. In column **S-box in Hex** the permuted [2] 4-bit Bent S-boxes are shown with the hexadecimal equivalents of their elements.

4. In column **DEs of BFs-Complement crypto S-box CSB(DBF1,DBF2,DBF3,DBF4)** DBF1 shows the decimal equivalent of 4th OPBF of the 4-bit Complement Bent S-boxes. Similarly DBF2, DBF3 and DBF4 show decimal equivalents of 3rd OPBF, 2nd OPBF and 1st OPBF of the same.

5. In column **Complement S-box in Hex** the permuted [2] 4-bit Complement Bent S-boxes are shown with the hexadecimal equivalents of their elements.

6. In columns **(1,2), (1,3), (1,4), (2,3), (2,4)** and **(3,4)** the decimal equivalents of the xor 4-bit BFs of the (DBF1, DBF2), (DBF1, DBF3), (DBF1, DBF4), (DBF2, DBF3), (DBF2, DBF4) and (DBF3, DBF4) respectively are shown. And immediate next **10s** are used to store the number of 1s under 1 and 0s under 0 of the xored 4-bit BFs respectively.

7. Here the column **88** is used to store the numbers of xored BFs that are balanced or have 8 1s and 8 0s in its binary output vector. Similarly column **97** and **A6** are used to store the numbers of xored BFs that are unbalanced and have 9 1s and 7 0s and 10 1s and 6 0s in its binary output vector respectively.

8. Here **L 0** and **D 0** shows numbers of 0s in LAT and DDT of the said 4-bit Bent S-boxes and their corresponding complement 4-bit Bent S-boxes respectively.

6. Results and discussion: In this analysis it is found that the numbers of 0s in LAT and DDT of the 4-bit Bent S-boxes and their corresponding 4-bit Complement Bent S-boxes are adequate to use the generated 4-bit Bent S-boxes in encryption and decryption algorithms of block ciphers. Since S-boxes are used in nonlinear substitution and many S-boxes can be used in a particular block cipher so the hurdle to use non-crypto 4-bit S-boxes in block ciphers can easily be overcome.

Conclusion: It can be concluded from the results that the non-crypto 4-bit S-boxes can be used in block ciphers. The Bent 4-bit S-boxes are the best option to replace crypto 4-bit S-boxes with the non-crypto 4-bit S-boxes. The said Bent 4-bit S-boxes have a very high security and very fine design methodology. So Bent non-crypto 4-bit S-boxes are the better choice than low secure crypto 4-bit S-boxes.

Acknowledgement. For this exhaustive work I would like to acknowledge my supervisors Dr. Ranjan Ghosh, Associate Professor, Institute of Radio Physics and Electronics, University of Calcutta and Prof. (Dr.) Amlan Chakrabarti Director, A K Choudhury School of Information Technology, University of Calcutta for their continuous encouragement and help. I would also like to acknowledge Prof. (Dr.) Gopa Sen, Head Dept. Institute of Radio Physics and Electronics, University of Calcutta for providing me with a nice and continuous infrastructure.

7. References:

1. Adams, Carlisle, Tavares, Stafford, "The structured design of cryptographically good S-boxes", J. Cryptology (1990) 344 vol. 3, pp : 27-41.

2. Dey S, Chakrabarti A, Ghosh R. 4-bit Boolean functions in generation and cryptanalysis of secure 4-bit crypto S-boxes. Security and Privacy. 2019; e90. Willey Periodicals Inc. DOI: https://doi.org/10.1002/spy2.90.

3. **Dey, S** and Ghosh, R. (2018) A Review of Existing 4-Bit Crypto S-Box Cryptanalysis Techniques and Two New Techniques with 4-Bit Boolean Functions for Cryptanalysis of 4-Bit Crypto S-Boxes*. Advances in Pure Mathematics, **8**, 272-306. ISSN Online: 2160-0384 ISSN Print: 2160-0368 DOI: **10.4236/apm.2018.83015.**

4. Dey, S and Ghosh, R, "A smart review and two new techniques using 4-bit Boolean functions for cryptanalysis of 4-bit crypto S-boxes.", Vol.40, issue.3, pp.1-19, International Journal of Computers and Applications, Taylor and Francis publishers, Year: 2018. ISSN. 1206-212X. DOI. **https://doi.org/10.1080/1206212X.2018.1504459**.

5. Feistel, H. "Block Cipher Cryptographic System", US Patent 3798359 (Filed June 30, 1971).

6. A. Sorkin, (1984). LUCIFER: a cryptographic algorithm. Cryptologia, **8**(1), 22–35, 1984.

7. Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC (1977).

8. Data Encryption Standard (DES), Federal Information Processing Standards Publication (FIPS PUB) 46-3, National Institute of Standards and Technology, Gaithersburg, MD (1999).

9. H.M.Heys. A tutorial on linear and differential cryptanlysis.cryptologia,26(2002),189-221.

10. H.M.Heys and S.E. Tavares, Substitution-permutation networks resistant to differential and linear cryptanalysis, Journal of Cryptology,9(1996),1-19.

Appendix:

Sl.No	BF (Dec)	BF (BInary)	10	L	CBF (Dec)	CBF (BInary)	10	L	ANF Coefficients	FO-SAC Mm	8 4 21-------3569AC--7BDE-F---SUM-------3569AC-7BDE--F--- SUM (SFO-SAC, SFO, MHO-SAC, MHO)
00001	00854	0000001101010110	6a	2	64681	1111110010101001	a6	4	C-0000-001100-0000-0	A6	1111-----111111-1111-1---011-----111111-1111-1---011
00002	00857	0000001101011001	6a	2	64678	1111110010100110	a6	4	C-0000-001101-0000-0	A6	1111-----111111-1111-1---011-----111111-1011-1---010
00003	00869	0000001101100101	6a	2	64666	1111110010011010	a6	4	C-0000-001110-0000-0	A6	1111-----111111-1111-1---011-----111111-1011-1---010
00004	00874	0000001101101010	6a	2	64661	1111110010010101	a6	4	C-0000-001111-0000-0	A6	1111-----111111-1111-1---011-----111111-1111-1---011
00005	00917	0000001110010101	6a	2	64618	1111110001101010	a6	4	C-0001-001111-0000-0	A6	1111-----111111-1111-1---011-----111111-1111-1---011
00006	00922	0000001110011010	6a	2	64613	1111110001100101	a6	4	C-0001-001110-0000-0	A6	1111-----111111-1111-1---011-----111111-1011-1---010
00007	00934	0000001110100110	6a	2	64601	1111110001011001	a6	4	C-0001-001101-0000-0	A6	1111-----111111-1111-1---011-----111111-1011-1---010
00008	00937	0000001110101001	6a	2	64598	1111110001010110	a6	4	C-0001-001100-0000-0	A6	1111-----111111-1111-1---011-----111111-1111-1---011
00009	01334	0000010100110110	6a	2	64201	1111101011001001	a6	4	C-0000-010010-0000-0	A6	1111-----111111-1111-1---011-----111111-1111-1---011
00010	01337	0000010100111001	6a	2	64198	1111101011000110	a6	4	C-0000-010011-0000-0	A6	1111-----111111-1111-1---011-----111111-1011-1---010

Table.2.1 Properties of 10 4-bit Bent BFs with their Complement 4-bit Bent BFs.

Sl No.	*DEs of BFs-crypto S-box SB(DBF1,DBF2,DBF3,DBF4)*	*S-box in Hex*	*DEs of BFs-complement crypto S-box CSB(DBF1,DBF2,DBF3,DBF4)*	*Complement S-box in Hex*	*(1,2)*	*10*	*(1,3)*	*10*	*(1,4)*	*10*	*(2,3)*	*10*	*(2,4)*	*10*	*(3,4)*	*10*	*Total 88 97 A6 L 0 D 0*
001.01	SB(00854,00857,00869,00874)	000000ff0f3c5a96	CSB(64681,64678,64666,64661)	ffffff00f0c3a569	00015	4c	00051	4c	00060	4c	00060	4c	00051	4c	00015	4c	00 00 00 102 165
001.02	SB(00857,00854,00869,00874)	000000ff0f3c965a	CSB(64678,64681,64666,64661)	ffffff00f0c369a5	00015	4c	00060	4c	00051	4c	00051	4c	00060	4c	00015	4c	00 00 00 102 165
001.03	SB(00854,00869,00857,00874)	000000ff0f5a3c96	CSB(64681,64666,64678,64661)	ffffff00f0a5c369	00051	4c	00015	4c	00060	4c	00060	4c	00015	4c	00051	4c	00 00 00 102 165
001.04	SB(00857,00869,00854,00874)	000000ff0f5a963c	CSB(64678,64666,64681,64661)	ffffff00f0a569c3	00060	4c	00015	4c	00051	4c	00051	4c	00015	4c	00060	4c	00 00 00 102 165
001.05	SB(00869,00854,00857,00874)	000000ff0f963c5a	CSB(64666,64681,64678,64661)	ffffff00f069c3a5	00051	4c	00060	4c	00015	4c	00015	4c	00060	4c	00051	4c	00 00 00 102 165
001.06	SB(00869,00857,00854,00874)	000000ff0f965a3c	CSB(64666,64678,64681,64661)	ffffff00f069a5c3	00060	4c	00051	4c	00015	4c	00015	4c	00051	4c	00060	4c	00 00 00 102 165
001.07	SB(00854,00857,00874,00869)	000000ff0f3c69a5	CSB(64681,64678,64661,64666)	ffffff00f0c3965a	00015	4c	00060	4c	00051	4c	00051	4c	00060	4c	00015	4c	00 00 00 102 165
001.08	SB(00857,00854,00874,00869)	000000ff0f3ca569	CSB(64678,64681,64661,64666)	ffffff00f0c35a96	00015	4c	00051	4c	00060	4c	00060	4c	00051	4c	00015	4c	00 00 00 102 165
001.09	SB(00854,00869,00874,00857)	000000ff0f693ca5	CSB(64681,64666,64661,64678)	ffffff00f096c35a	00051	4c	00060	4c	00015	4c	00015	4c	00060	4c	00051	4c	00 00 00 102 165
001.10	SB(00857,00869,00874,00854)	000000ff0f69a53c	CSB(64678,64666,64661,64681)	ffffff00f0965ac3	00060	4c	00051	4c	00015	4c	00015	4c	00051	4c	00060	4c	00 00 00 102 165
001.11	SB(00869,00854,00874,00857)	000000ff0fa53c69	CSB(64666,64681,64661,64678)	ffffff00f05ac396	00051	4c	00015	4c	00060	4c	00060	4c	00015	4c	00051	4c	00 00 00 102 165
001.12	SB(00869,00857,00874,00854)	000000ff0fa5693c	CSB(64666,64678,64661,64681)	ffffff00f05a96c3	00060	4c	00015	4c	00051	4c	00051	4c	00015	4c	00060	4c	00 00 00 102 165
001.13	SB(00854,00874,00857,00869)	000000ff0f5a69c3	CSB(64681,64661,64678,64666)	ffffff00f0a5963c	00060	4c	00015	4c	00051	4c	00051	4c	00015	4c	00060	4c	00 00 00 102 165
001.14	SB(00857,00874,00854,00869)	000000ff0f5ac369	CSB(64678,64661,64681,64666)	ffffff00f0a53c96	00051	4c	00015	4c	00060	4c	00060	4c	00015	4c	00051	4c	00 00 00 102 165
001.15	SB(00854,00874,00869,00857)	000000ff0f695ac3	CSB(64681,64661,64666,64678)	ffffff00f096a53c	00060	4c	00051	4c	00015	4c	00015	4c	00051	4c	00060	4c	00 00 00 102 165
001.16	SB(00857,00874,00869,00854)	000000ff0f69c35a	CSB(64678,64661,64666,64681)	ffffff00f0963ca5	00051	4c	00060	4c	00015	4c	00015	4c	00060	4c	00051	4c	00 00 00 102 165

001.17 SB(00869,00874,00854,00857) 000000ff0fc35a69 CSB(64666,64661,64681,64678) ffffff00f03ca596 00015 4c 00051 4c 00060 4c 00060 4c 00051 4c 00015 4c 00 00 00 102 165
001.18 SB(00869,00874,00857,00854) 000000ff0fc3695a CSB(64666,64661,64678,64681) ffffff00f03c96a5 00015 4c 00060 4c 00051 4c 00051 4c 00060 4c 00015 4c 00 00 00 102 165
001.19 SB(00874,00854,00857,00869) 000000ff0f96a5c3 CSB(64661,64681,64678,64666) ffffff00f0695a3c 00060 4c 00051 4c 00015 4c 00015 4c 00051 4c 00060 4c 00 00 00 102 165
001.20 SB(00874,00857,00854,00869) 000000ff0f96c3a5 CSB(64661,64678,64681,64666) ffffff00f0693c5a 00051 4c 00060 4c 00015 4c 00015 4c 00060 4c 00051 4c 00 00 00 102 165
001.21 SB(00874,00854,00869,00857) 000000ff0fa596c3 CSB(64661,64681,64666,64678) ffffff00f05a693c 00060 4c 00015 4c 00051 4c 00051 4c 00015 4c 00060 4c 00 00 00 102 165
001.22 SB(00874,00857,00869,00854) 000000ff0fa5c396 CSB(64661,64678,64666,64681) ffffff00f05a3c69 00051 4c 00015 4c 00060 4c 00060 4c 00015 4c 00051 4c 00 00 00 102 165
001.23 SB(00874,00869,00854,00857) 000000ff0fc396a5 CSB(64661,64666,64681,64678) ffffff00f03c695a 00015 4c 00060 4c 00051 4c 00051 4c 00060 4c 00015 4c 00 00 00 102 165
001.24 SB(00874,00869,00857,00854) 000000ff0fc3a596 CSB(64661,64666,64678,64681) ffffff00f03c5a69 00015 4c 00051 4c 00060 4c 00060 4c 00051 4c 00015 4c 00 00 00 102 165

Table.4.1 BIC, LC and DC analysis of 4! or 24 permuted non-crypto 4-bit S-boxes.