Analysis of the Avalanche Effect of the AES S Box

Hui Shi Yuanqing Deng Yu Guan
Institute of Science
PLA University of Science & Technology
Nanjing China

***Abstract*—AS the unique nonlinear structure in most block ciphers, S-box accounts for the AES algorithm's security. Firstly, this paper introduces the cryptographic properties of the S box. Then a detail analysis of the avalanche effect of the AES S box and inverse S box are made. Lastly, the paper indicates that AES S box and inverse S box indeed have the good avalanche effect by detailed data.**

Keywords- Cryptographic property; AES; Avalanche Effect; S Box; Inverse S Box

I. INTRODUCTION

AS the unique nonlinear structure in most block ciphers, S-box accounts for the AES algorithm's security. When design and analysis AES[1-4], the cryptographic properties of S box must be considered, such as Balanceness, Strict Avalanche Criterion, Nonlinearity, Orthogonality, Differential Property, Algebraic Order, and so on.

A. The cryptographic properties of S box[5-6]

1) Balanceness

Define 1: $\boldsymbol{s}:\boldsymbol{GF}(2)^8\rightarrow\boldsymbol{GF}(2)^8$

When the input value is ergodic, the number of input "1" is equal to the number of output "0", and s meets balanceness.

2) Strict Avalanche Criterion[8]

Define 2: $\boldsymbol{s}:\boldsymbol{GF}(2)^8\rightarrow\boldsymbol{GF}(2)^8$

A change in one bit of input bits of S-box should produce a change in half of output bits of S-box.

3) Nonlinearity

Define 3: $\boldsymbol{S}(\boldsymbol{x})=(\boldsymbol{s}_1(\boldsymbol{x}),\ldots,\boldsymbol{s}_{\mathrm{m}}(\boldsymbol{x})),\boldsymbol{m}\le\boldsymbol{n},$

$\boldsymbol{NF}=\min\limits_{0\neq\boldsymbol{u}\in\boldsymbol{GF}(2)^{\boldsymbol{m}}\,\boldsymbol{l}(\boldsymbol{x})\in\boldsymbol{L}_{\boldsymbol{n}}[\boldsymbol{x}]}\boldsymbol{d}(\boldsymbol{u}\bullet\boldsymbol{S}(\boldsymbol{x}),\boldsymbol{l}(\boldsymbol{x}))$ is nonlinearity of S(x)[9].

4) Orthogonality

Define 4: $\boldsymbol{S}(\boldsymbol{x})=(\boldsymbol{s}_1(\boldsymbol{x}),\ldots,\boldsymbol{s}_{\mathrm{m}}(\boldsymbol{x})),\boldsymbol{m}\le\boldsymbol{n},$

For any $\boldsymbol{\beta}\in\boldsymbol{GF}(2)^{\boldsymbol{m}}$, there are just $2^{\boldsymbol{n}-\boldsymbol{m}}$ elements in assemble $\{\boldsymbol{\alpha}|\boldsymbol{\alpha}\in\boldsymbol{GF}(2)^{\boldsymbol{n}},\boldsymbol{S}(\boldsymbol{\alpha})=\boldsymbol{\beta}\}$, it says $\boldsymbol{S}(\boldsymbol{x})$ is orthogonal.

5) Differential Property

Differential uniformance and Robust degrees indicate that S box can fight the differential cryptanalysis attack with good difference characteristics.

6) Algebraic Order

Define 5: $\boldsymbol{S}(\boldsymbol{x})=(\boldsymbol{s}_1(\boldsymbol{x}),\ldots,\boldsymbol{s}_{\mathrm{m}}(\boldsymbol{x})):\boldsymbol{GF}(2)^{\mathrm{n}}\rightarrow\boldsymbol{GF}(2)^{\mathrm{m}}$

$$\boldsymbol{D}(\boldsymbol{S})=\min\{\deg(\boldsymbol{\beta}\bullet\boldsymbol{S})|\boldsymbol{\beta}\neq 0,\boldsymbol{\beta}\in\boldsymbol{GF}(2)^{\boldsymbol{m}}\}$$

$$=\min\{\deg(\sum_{i=1}^{m}\boldsymbol{b}_{\mathrm{i}}\boldsymbol{s}_{\mathrm{i}}(\boldsymbol{x})|(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{\boldsymbol{m}}=\boldsymbol{\beta}\neq 0),(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{\boldsymbol{m}})\in\boldsymbol{GF}(2)^{\boldsymbol{m}}\}$$

$\boldsymbol{D}(\boldsymbol{S})$ is algebraic order of $\boldsymbol{S}(\boldsymbol{x})$.

In a way, the number of algebraic order gives S box linear complexity. The more algebraic order, it shows that S box has higher linear complexity, the less easy to linear expressions approximation.

For all of the cryptographic properties, the avalanche effect of S box is especially important and we just discuss the avalanche effect of AES.

II. THE TEST OF AVALANCHE EFFECT OF S BOX

The Avalanche Effect is proposed by Feistel. The Avalanche Effect of S Box: When an input bit of S box makes the change, half of the output bits will make the change. The Avalanche Effect is used to indicate the randomness of S box when input has a change. It must be taken into account when S box is designed.

A. Changed Probability of output bit.

The changed probability of output bit of the AES S-box[11-14] and inverse S-box are shown in TABLE Ⅰ.The first column of the table shows the input bits of the S-box and the inverse S-box. The second column of the table shows the changed probability of every output bit of the AES S-box and inverse S-box, which are both almost equal to 0.5. It can be concluded that the AES S-box and inverse S-box have a very good property.

TABLE I. THE CHANGED PROBABILITY OF OUTPUT BIT

Input	Changed Probability of Output Bit		Input	Changed Probability of Output Bit

978-1-4577-0536-6/11/$26.00 ©2011 IEEE

	AES S-Box / Inverse S-Box			AES S-Box / Inverse S-Box
00000000	0.46875/0.421875		10000000	0.53125/0.546875
00000001	0.59375/0.5625		10000001	0.5/0.484375
00000010	0.390625/0.640625		10000010	0.59375/0.546875
00000011	0.4375/0.625		10000011	0.578125/0.4375
00000100	0.4375/0.53125		10000100	0.5/0.5625
00000101	0.5/0.484375		10000101	0.484375/0.46875
00000110	0.421875/0.5625		10000110	0.484375/0.53125
00000111	0.53125/0.546875		10000111	0.515625/0.578125
00001000	0.484375/0.5625		10001000	0.390625/0.5
00001001	0.515625/0.578125		10001001	0.546875/0.4375
00001010	0.40625/0.546875		10001010	0.484375/0.53125
00001011	0.40625/0.515625		10001011	0.453125/0.4375
00001100	0.5/0.515625		10001100	0.578125/0.5625
00001101	0.484375/0.46875		10001101	0.453125/0.453125
00001110	0.5/0.4375		10001110	0.5625/0.40625
00001111	0.546875/0.515625		10001111	0.4375/0.515625
00010000	0.4375/0.453125		10010000	0.4375/0.546875
00010001	0.5625/0.578125		10010001	0.5625/0.5625
00010010	0.515625/0.515625		10010010	0.625/0.421875
00010011	0.515625/0.46875		10010011	0.453125/0.484375
00010100	0.46875/0.5		10010100	0.515625/0.546875
00010101	0.609375/0.46875		10010101	0.546875/0.390625
00010110	0.5625/0.484375		10010110	0.59375/0.515625
00010111	0.515625/0.453125		10010111	0.421875/0.453125
00011000	0.578125/0.5		10011000	0.484375/0.625
00011001	0.5625/0.578125		10011001	0.546875/0.421875
00011010	0.421875/0.484375		10011010	0.59375/0.609375
00011011	0.546875/0.484375		10011011	0.5/0.5
00011100	0.5/0.46875		10011100	0.484375/0.609375
00011101	0.53125/0.46875		10011101	0.421875/0.5
00011110	0.5/0.453125		10011110	0.5/0.484375
00011111	0.515625/0.5		10011111	0.453125/0.484375
00100000	0.421875/0.453125		10100000	0.4375/0.578125
00100001	0.453125/0.515625		10100001	0.546875/0.390625
00100010	0.46875/0.53125		10100010	0.4375/0.5
00100011	0.640625/0.46875		10100011	0.453125/0.484375
00100100	0.46875/0.5		10100100	0.5/0.578125
00100101	0.5/0.625		10100101	0.546875/0.484375
00100110	0.484375/0.484375		10100110	0.46875/0.546875
00100111	0.5/0.578125		10100111	0.46875/0.453125
00101000	0.4375/0.453125		10101000	0.46875/0.484375
00101001	0.515625/0.515625		10101001	0.46875/0.5625
00101010	0.46875/0.578125		10101010	0.46875/0.5625
00101011	0.484375/0.421875		10101011	0.5/0.46875
00101100	0.375/0.515625		10101100	0.5/0.484375
00101101	0.640625/0.453125		10101101	0.453125/0.5
00101110	0.4375/0.40625		10101110	0.515625/0.53125
00101111	0.5/0.5		10101111	0.484375/0.484375
00110000	0.5/0.484375		10110000	0.515625/0.5625
00110001	0.421875/0.484375		10110001	0.546875/0.546875
00110010	0.4375/0.53125		10110010	0.484375/0.53125
00110011	0.453125/0.5		10110011	0.484375/0.546875
00110100	0.5/0.46875		10110100	0.484375/0.59375
00110101	0.453125/0.59375		10110101	0.59375/0.546875
00110110	0.546875/0.515625		10110110	0.53125/0.578125
00110111	0.578125/0.515625		10110111	0.5/0.484375
00111000	0.515625/0.53125		10111000	0.46875/0.546875
00111001	0.484375/0.453125		10111001	0.5/0.359375
00111010	0.4375/0.53125		10111010	0.46875/0.578125
00111011	0.40625/0.484375		10111011	0.46875/0.515625
00111100	0.625/0.515625		10111100	0.5625/0.484375
00111101	0.546875/0.46875		10111101	0.5625/0.53125
00111110	0.4375/0.546875		10111110	0.453125/0.453125
00111111	0.59375/0.59375		10111111	0.53125/0.515625
01000000	0.484375/0.4375		11000000	0.5625/0.640625
01000001	0.609375/0.375		11000001	0.5/0.53125
01000010	0.484375/0.53125		11000010	0.453125/0.640625
01000011	0.53125/0.453125		11000011	0.4375/0.546875
01000100	0.421875/0.578125		11000100	0.484375/0.546875
01000101	0.484375/0.546875		11000101	0.53125/0.53125
01000110	0.59375/0.53125		11000110	0.5/0.59375
01000111	0.5625/0.484375		11000111	0.421875/0.5
01001000	0.5/0.421875		11001000	0.484375/0.5
01001001	0.46875/0.421875		11001001	0.484375/0.59375
01001010	0.5/0.4375		11001010	0.53125/0.546875
01001011	0.453125/0.453125		11001011	0.484375/0.46875
01001100	0.515625/0.609375		11001100	0.515625/0.59375
01001101	0.59375/0.53125		11001101	0.53125/0.546875
01001110	0.5/0.53125		11001110	0.484375/0.53125

01001111	0.5/0.515625		11001111	0.4375/0.546875
01010000	0.421875/0.359375		11010000	0.421875/0.59375
01010001	0.484375/0.390625		11010001	0.59375/0.515625
01010010	0.4375/0.484375		11010010	0.515625/0.5625
01010011	0.546875/0.453125		11010011	0.53125/0.578125
01010100	0.515625/0.421875		11010100	0.546875/0.53125
01010101	0.546875/0.40625		11010101	0.546875/0.453125
01010110	0.5625/0.453125		11010110	0.53125/0.59375
01010111	0.609375/0.5625		11010111	0.421875/0.484375
01011000	0.4375/0.515625		11011000	0.40625/0.578125
01011001	0.578125/0.484375		11011001	0.546875/0.5
01011010	0.515625/0.453125		11011010	0.578125/0.53125
01011011	0.453125/0.40625		11011011	0.515625/0.5625
01011100	0.40625/0.53125		11011100	0.5625/0.515625
01011101	0.484375/0.390625		11011101	0.578125/0.453125
01011110	0.53125/0.4375		11011110	0.484375/0.4375
01011111	0.5/0.546875		11011111	0.390625/0.4375
01100000	0.5/0.390625		11100000	0.453125/0.515625
01100001	0.421875/0.40625		11100001	0.4375/0.4375
01100010	0.46875/0.59375		11100010	0.46875/0.46875
01100011	0.5/0.4375		11100011	0.53125/0.609375
01100100	0.4375/0.375		11100100	0.46875/0.40625
01100101	0.40625/0.484375		11100101	0.546875/0.46875
01100110	0.5/0.546875		11100110	0.546875/0.4375
01100111	0.453125/0.4375		11100111	0.4375/0.515625
01101000	0.5625/0.546875		11101000	0.546875/0.53125
01101001	0.515625/0.4375		11101001	0.59375/0.5
01101010	0.546875/0.578125		11101010	0.5625/0.515625
01101011	0.53125/0.40625		11101011	0.625/0.5625
01101100	0.453125/0.609375		11101100	0.609375/0.46875
01101101	0.53125/0.46875		11101101	0.40625/0.484375
01101110	0.59375/0.59375		11101110	0.625/0.5
01101111	0.59375/0.421875		11101111	0.5625/0.546875
01110000	0.46875/0.484375		11110000	0.578125/0.640625
01110001	0.421875/0.453125		11110001	0.46875/0.515625
01110010	0.46875/0.515625		11110010	0.4375/0.5
01110011	0.484375/0.5625		11110011	0.359375/0.546875
01110100	0.453125/0.515625		11110100	0.59375/0.546875
01110101	0.46875/0.484375		11110101	0.578125/0.46875
01110110	0.53125/0.484375		11110110	0.5625/0.546875
01110111	0.5625/0.40625		11110111	0.546875/0.421875
01111000	0.625/0.484375		11111000	0.546875/0.5
01111001	0.5/0.546875		11111001	0.546875/0.328125
01111010	0.5625/0.640625		11111010	0.53125/0.53125
01111011	0.59375/0.40625		11111011	0.453125/0.546875
01111100	0.5/0.453125		11111100	0.515625/0.546875
01111101	0.546875/0.421875		11111101	0.453125/0.46875
01111110	0.4375/0.53125		11111110	0.484375/0.4375
01111111	0.515625/0.53125		11111111	0.453125/0.453125
ave	0.503296/0.505737			

B. Test on the avalance effect of the AES S box and inverse S box

1) AES S-Box

The test data of avalanche effect on the AES S-box are shown in TABLE Ⅱ. The first column of the table shows the changed input bits of the S-box. The changed average number of output bits of the S-box can be found when every bit of the input data respectively changed from the second to the ninth column of the TABLE Ⅱ.

TABLE II. THE AVALANCHE EFFECT OF S BOX

X Var	Total bits of changed Y（$y_8y_7y_6y_5y_4y_3y_2y_1$）									
	y_8	y_7	y_6	y_5	y_4	y_3	y_2	y_1	Sum	Ave
X_8	112	140	140	128	116	128	128	120	1012	126.5
X_7	112	128	140	136	136	128	140	132	1052	131.5
X_6	128	140	136	139	121	140	124	112	1040	130
X_5	132	112	136	136	140	140	136	132	**1064**	**133**
X_4	112	136	136	120	136	136	136	132	1044	130.5
X_3	136	136	120	136	132	136	128	112	1036	129.5
X_2	116	120	112	140	144	128	128	128	1016	127
X_1	120	112	140	140	124	120	132	116	**1004**	**125.5**

2) AES Inverese S-Box

The test data of avalanche effect on the AES Inverse S-box are shown in TABLE Ⅲ. The first column of the table shows the changed input bits of the inverse S-box. The changed average number of output bits of the inverse S-box can be found when every bit of the input data respectively changed from the second to the ninth column of the TABLE Ⅲ.

TABLE III. THE AVALANCHE EFFECT OF INVERSE S BOX

X Var	Total bits of changed Y（$y_8y_7y_6y_5y_4y_3y_2y_1$）									
	y_8	y_7	y_6	y_5	y_4	y_3	y_2	y_1	Sum	Ave
X_8	132	122	134	124	134	134	144	132	**1056**	**132**
X_7	124	136	136	118	130	116	136	134	1030	128.75
X_6	138	136	140	120	118	130	134	114	1030	128.75
X_5	136	140	126	128	130	118	128	116	1022	127.75
X_4	140	128	136	128	114	122	136	136	1040	130
X_3	128	136	128	144	118	126	132	132	1044	130.5
X_2	136	128	116	124	126	146	124	120	1020	127.5
X_1	128	116	124	116	142	114	132	132	**1004**	**125.5**

From table Ⅱ and table Ⅲ, we can obtain the following conclusions：

3) The avalanche effect of S Box

when X_5 changed, the sum changed bits of Y is the biggest. The total changed bits are 1064, and the average is 133, bigger than half of 256 bits (that is 128 bits); When X_1 changed, the total changed bits of Y are the least. The total changed bits are 1004, and the average is 125.5, almost half of 256 bits. The test result indicated that the S box indeed has the good input avalanche effect.

4) The avalanche effect of Inverse S Box

when X_8 changed, the sum changed bits of Y is the biggest. The total changed bits are 1056, and the average is 132, bigger than half of 256 bits (that is 128 bits); When X_1 changed, the sum changed bits of Y are the least. The total changed bits are 1004，and the average is 125.5, almost half of 256 bits. The test result indicated that the Inverse S box indeed has the good input avalanche effect.

III. CONCLUSION

S-box is the only non-linear structure of the block cipher, providing the nonlinearity and the security. When design and analysis AES, the cryptographic properties of S box must be considered, especially the avalanche effect. We can conclude that AES S-box and inverse S-box both have the good avalanche property with the detailed data.

REFERENCES

[1] Daemen J,Rijmen J.AES proposal: Rijndael.NIST'1998. Ventura CA, USA, 1998.1-45.

[2] Joan Daemen and Vincent Rijmen, Dawu Gu, Shengbo Xu translation. AES Algorithm－the design of Rijndael . Publishing House of Tsinghua University, 2003.03.

[3] William Stalling(US) , Ming Yang translation and so on . Cryptography and Network Security Principles and Practices (Fourth Edition)[M]. Beijing: Publishing House of Electronics Industry, 2006.

[4] Xiangdong Hu, Qinfang Wei. Application Cryptology Course, [M]. Beijing: Publishing House of Electronics Industry. 2005.

[5] Jingwei Liu, Baodian Wei, jiqiang Lu, Xinmei Wang. "Analysis of the cryptographic properties of the AES S-box",Journal OF Xindian University [C],pp:255-259, 2004.

[6] Xuewang Zhang, Hong Jiang, Changjun Xiao, Liangyou Huang. "Study on Analysis of AES's S-Box and its Improvement",Information Safety [C],pp:51-53, 2009.

[7] E.Bihan, O.Dunkelman, N.Keller, "Related-Key Impossible Differential Attacks on 8-Round AES-192" , Topics in Cryptology-CT-RSA 2006, Plncs3860, pp:21-33, Springer-Verlag, 2006.

[8] N.T.Courtois, J.Pieprzyk, "Cryptanalysis of Block Cipher with Overdefined Systems of Equation" , Advances in Cryptology-CRYPTO 2002, LNCS2501, pp:267-287, Springer-Verlag, 2002.

[9] Webster A F, Tavares S E. On the Design of S-Boxes[A]. Advances in Cryptology:CRYPOTO'85[C]. Berlin: Springer-Verlag,1985.224-234.

[10] Nyberg K. Perfect Nonlinear S-Boxes[A]. Advances in Cryptology: EUROCRYPTO'91[C]. Berlin: Springer-Verlag,1991.378-386.

[11] Wentao Zhang, lei Zhang, Wenling Wu etc. "Related-Key Differential-linear attacks on Reduced AES-192", Progress in Crypology-INDOCRYPT 2007, CS 4859, pp:73-85, Springer-Verlag, 2007.

[12] J.Kim, S.Hong, B.Preneel, "Related-Key Rectangle Attacks on Reduced AES-192 and AES-256", Fast Software Encrytion-FSE 2007, LNCS 4593, pp:2225-241, Springer-Verlag, 2007.

[13] G.N.Krishnamurthy, V.ramaswamy, "Making AES Stronger:AES with Key Dependent S-Box", IJCSNS international Journal of Computer Science and Network Security, Vol.8 No.9, pp:388-398, September 2008.

[14] Jiqiang Lv, O.Dunkelman, N.Keller,etc. "New Impossible Differential Attacks on AES", International Conference on Cryptology-INDOCRYPT 2008, LNCS 5365 pp:279-293, Springer-Verlag, 2008.

[15] Yuanqing Deng, Jing Gong, Hui Shi, Concise Course on Cryptography, Publishing House of Qinghua University, 2011.