The Differential Cryptanalysis of an AES Finalist–Serpent

X.Y.Wang*† L.C.K.Hui* K.P.Chow* C.F.Chong* W.W.Tsang*
H.W.Chan*

Technical Report TR-2000-04
April 2000
*Department of Computer Science & Information Systems
The University of Hong Kong
Pokfulam, Hong Kong

†Department of Mathematics
Shandong University
Jinan 250100 PRC

hui@csis.hku.hk

Abstract

Serpent is one of the five AES finalists. In our paper, we give some differentials about Serpent, two of the differentials are a 5-round differential with the probability of $\frac{1}{2^{61}}$ and a 6-round differential with the probability of $\frac{1}{2^{97}}$. The best known differential before our paper is a 5-round differential with the probability of $\frac{1}{2^{80}}$ given in [9].

Additionally, we provide all the possible best differentials for some cases about Serpent. From these best differentials, we conclude that the 16-round best differential is not higher than $\frac{1}{2^{118}}$, and that the 17-round differential is less than $\frac{1}{2^{126}}$.

1 Introduction

The US National Institute of Standards and Technology has been working with industry and cryptographic community to develop an Advanced Encryption Standard(AES). So far, three AES Candidate Conference had been held.

In the first AES Candidate Conference (AES1), fifteen algorithm had been submitted.

In the second AES Candidate Conference (AES2), there are five algorithms selected as finalists. The AES finalist candidate algorithms are MARS, RC6, Rijndael, Serpent [1, 2], and Twofish.

And the third AES Candidate Conference (AES3) had just been closed on April 14, 2000 in New York, NY, USA. Submitters of the AES finalists had been invited to attend and gave statements on their algorithms. All five AES finalists seem secure, and no known valid attacks are presented.

In our paper, we are interested in analyzing the security of Serpent against differential attack. Our main aim is to describe the bound about the best differentials of Serpent, without concerning the attacks of these differential on Serpent.

Two groups have made some security analysis of Serpent. One group is the designers of Serpent. In their design, they gave a bound table about differential estimation within 7 rounds, and guessed that the 28-round best differential is not higher than 2^{-120}. They only gave this as a conjecture and did not provide any concrete differential examples.

The other group is T. Kohno etal. [9]. In their paper, they gave a 5-round differential with a probability of $\frac{1}{2^{80}}$. Using this differential, they gave some attack results about reduced Serpent variants.

In our paper, we first give some differentials about Serpent. Among these differentials, a 5-round differential occurs with the probability of $\frac{1}{2^{61}}$, a 6-round differential occurs with the probability of $\frac{1}{2^{97}}$. The best known differential before our paper is a 5-round differential with the probability of $\frac{1}{2^{80}}$.

Second, we analyze the possible best differentials for some cases about Serpent. From these analysis results, we conclude that the 16-round best differential is less than $\frac{1}{2^{118}}$, and the 17-round best differential is less than $\frac{1}{2^{126}}$.

2 The Description of Serpent

Serpent is a 32-round SP-network operating on four 32-bit words, thus giving a block size of 128 bits. Serpent involves 8 different S-boxes (S_i, $i = 0, 1, ...7$). The indices of the bits are counted from 0 to bit 31 one 32-bit word. 0 to bit 127 in 128-bit blocks, 0 to bit 255 in 256-bit keys. The first word (word 0) is the least significant word, and the last word is the most significant, where bit 0 is the least significant bit of word 0.

Serpent encrypts a 128-bit plaintext P to a 128-bit ciphertext C in 32 rounds under the control of 33 128-bit subkeys $K_0, ...k_{32}$. These subkeys are

deduced from a 256-bit key. Because the generation of these subkeys have no relation with our analysis, we don't give it's details here.

The encryption algorithm is described as follows:

$$B_0 := IP(P)$$
$$B_{i+1} := R_i(B_i)$$
$$C := FP(B_{32})$$

where

$$R_i(B_i) := IP(L(FP(S(B_i \oplus K_i)))), i = 0, 1, 2, ...30$$
$$R_i(B_i) := S_i(B_i \oplus K_i) \oplus K_{32}, i = 31$$

IP and FP are two inverse permutations such that:

IP:

$$b_k \longrightarrow b_{4k}$$
$$b_{k+32} \longrightarrow b_{4k+1}$$
$$b_{k+64} \longrightarrow b_{4k+2}$$
$$b_{k+96} \longrightarrow b_{4k+3}$$

FP:

$$b_{4k} \longrightarrow b_k$$
$$b_{4k+1} \longrightarrow b_{k+32}$$
$$b_{4k+2} \longrightarrow b_{k+64}$$
$$b_{4k+3} \longrightarrow b_{k+96}$$

where $k = 0, 1, 2, ...31$

$X = (X_0, X_1, X_2, X_3)$, $X_0 = (b_0, b_1, b_2, ..b_{31})$ is the first (least significant) of X. $X_3 = (b_{96}, b_{97}, ...b_{127})$ is the fourth word (most significant) of X

L is the following linear transformation:

$$X_0 := X_0 <<< 13$$
$$X_2 := X_2 <<< 3$$
$$X_1 := X_1 \oplus X_0 \oplus X_2$$
$$X_3 := X_3 \oplus X_2 \oplus X_0 << 3$$
$$X_1 := X_1 <<< 1$$

$$X_3 := X_3 <<< 7$$

$$X_0 := X_0 \oplus X_1 \oplus X_3$$

$$X_2 := X_2 \oplus X_3 \oplus (X_1 << 7)$$

$$X_0 := x_0 <<< 5$$

$$X_2 := X_2 <<< 22$$

Output

$$L(X) := X0, X_1, X_2, X_3$$

Each round of Serpent can be simplified as two steps: one in the S-boxes, and the other is a linear transformation table: $LT(X) = IP(L(FP(X)))$. LT is given in the appendix of [1].

3 Some Notations and Conclusions about Serpent

Notations: In the remainer of the paper, we use $X = (x_0, x_1, ...x_{31})$ to denote an intermediate difference in each step. $x_0, x_1, ..., x_{31}$ are 32 nibble differences. x_0 is the least significant nibble difference, x_1 is the second nibble difference, and x_{31} is the most significant nibble difference.

$(b_0, b_1, ...b_{127})$ denotes 128-bits of X. b_0, b_1, b_2, b_3 is the left four bits, also is the four bits of x_0. $b_{124}, b_{125}, b_{126}, b_{127}$ is the most four bits (four bots of x_{31}).

(X_0, X_1, X_2, X_3) is four words in the linear transformation. It is known that: $(b_0, b_1, ...b_{127}) \xrightarrow{FP} (X_0, X_1, X_2, X_3)$, where $X_0 = (b_0, b_4, ...b_{4i}, ...b_{124}))$,..... $X_3 = (b_3, b_7, ...b_{4i+3}, ...b_{127}))$.

For some difference $X = (x_0, x_1, ...x_{31})$, there are t active S-boxes implies that, there are only t non-zero nibble difference, all other nibble differences are zero [3, 7].

The following give some kinds of one-round characteristics. Some cases cause the active S-boxes expansion in the next round, and some cause the active S-boxes reduction.

Property 1: If input difference of round k only has one active S-box, then the output difference in round k at least has two nonzero nibble differences.

Proof: This can be easily proved by looking for the linear transformation table in [1].

Table 1-table 3 give three examples for this kind of characteristic. Table 1 and table 3 are two examples that an active S-box in i-th round causes two active S-boxes in the next round.

Input	x_i=7	Pr
S_0	$x_i = 2$	$\frac{1}{2^3}$
LT	$x_{i+6} = 1$,$x_{i+1} = 2$, $x_{i+30} = 4$	1

Table 1: One-round Characteristic ($0 \leq i < 25$) with S_0 Boxes

Table 1 show that, if the input difference only has the nonzero difference nibble $x_i = 7$, then after applying S-box S_0, $x_i = 2$ holds with the probability $\frac{1}{2^3}$. The output difference has three nonzero nibbles: $x_{i+6} = 1$,$x_{i+1} = 2$, $x_{i-2} = 4$.

Proof of Table 1: We can easily prove the table 1 in the following. From the differential distribution of S_0, we know $x_i = 7 \xrightarrow{S_0} x_i = 2$ holds with the probability of $\frac{1}{2^3}$. It is:

$$(b_{4i} = 1, b_{4i+1} = 1, b_{4i+2} = 1, b_j = 0, j \neq i) \xrightarrow{S_0, \frac{1}{2^3}} (b_{4i+1} = 1, b_j = 0, j \neq i)$$

So,

$$(b_{4i+1} = 1, b_j = 0, j \neq i) \xrightarrow{FP} (X_0, X_1, X_2, X_3)$$

Where X_1 only has one nonzero bit $b_i = 1$, all other bits and all the bits of other X_k are zero.

After the linear transformation (table 2), we know:

$$(X_0, X_1, X_2, X_3) \xrightarrow{L} (X'_0, X'_1, X'_2, X'_3)$$

Where only the $b_{i+6} = 1$ in X'_0, $b_{i+1} = 1$ in X'_1, $b_{i+30} = 1$ in X'_2, and all other bits are zero.

Finally

$$(X'_0, X'_1, X'_2, X'_3) \xrightarrow{IP} (x_{i+1} = 2, x_{i+6} = 1, x_{i+30} = 4, x_j = 0, j \neq i+1, i+6, i+30)$$

This completes the proof.

This technique of proof can be used to deduce all other differentials in this paper.

Property 2: If input difference of round k only has two active S-boxs: $(i+10)$ and $(i+7)$ S-boxes, the output difference in round k may have one nonzero nibble difference.

The following are some examples (table 4 to table 5) for this kind of characteristic.

Input	$x_i = 7$	Pr
S_0	$x_i = 2$	$\frac{1}{2^3}$
LT	$x_{i+6} = 1$,$x_{i+1} = 2$	1

Table 2: One-round Characteristic ($31 \geq i > 25$) with S_0 Boxes

Input	$x_i = 13$	Pr
S_0	$x_i = 8$	$\frac{1}{2^2}$
LT	$x_{i+7} = 8$, $x_{i+12} = 1$, $x_{i+29} = 4$	1

Table 3: One-round Characteristic with S_0 Boxes

Input	$x_{i+10} = 10$,$x_{i+7} = 12$	Pr
S_0	$x_{i+10} = 10$,$x_{i+7} = 4$	$\frac{1}{2^4}$
LT	$x_i = 4$	1

Table 4: One-round Characteristic with S_0 Boxes

Input	$x_{i+10} = 9$,$x_{i+7} = 14$	Pr
S_0	$x_{i+10} = 10$,$x_{i+7} = 4$	$\frac{1}{2^5}$
LT	$x_i = 4$	1

Table 5: One-round Characteristic with S_1 Boxes

Lemma 3 All the S-boxes satisfy the following property: for any two nibbles x and y, if the input difference of one S-box is x, the output difference of the S-box equal to y with nonzero probability , the probability is $\frac{1}{2^2}$ or $\frac{1}{2^3}$.

Proof: See the generation of S-boxes [1] or see the S-boxes differential distributions in table 29-table 36 in the appendix.

4 Some Truncated Differentials about Serpent

[9] gave a 5-round differential with the probability of $\frac{1}{2^{80}}$ (see table 6). The differential is from round 2 to round 6 in the original serpent. This differential can be used to attack 6-round serpent variants with about 2^{90} serpent six-round encryptions.

R		Differences	Pr
I		$x_0 = 14, x_4 = 10, x_6 = 13, x_7 = 2, x_{18} = 12, x_{31} = 13$	
R_1	S_1	$x_0 = 8, x_4 = 4, x_6 = 2, x_7 = 10, x_{18} = 1,\ x_{31} = 2$	$\frac{1}{2^{13}}$
	LT	$x_4 = 5, x_7 = 10$	1
R_2	S_2	$x_4 = 4, x_7 = 10$	$\frac{1}{2^5}$
	LT	$x_{29} = 4$	1
R_3	S_3	$x_{29} = 10$	$\frac{1}{2^3}$
	LT	$x_3 = 1, x_4 = 8, x_9 = 1, x_{26} = 4, x_{30} = 2$	1
R_4	S_4	$x_3 = 14, x_4 = 12, x_9 = 7, x_{26} = 3, x_{30} = 6$	$\frac{1}{2^{10}}$
	LT	$x_0 = 13, x_2 = 6, x_3 = 4, x_4 = 3, x_5 = 1, x_7 = 3, x_8 = 8, x_9 = 5, x_{10} = 14$ $x_{11} = 8, x_{13} = 11, x_{14} = 8, x_{16} = 1, x_{17} = 8, x_{19} = 9, x_{20} = 4, x_{22} = 5$ $x_{23} = 6, x_{24} = 1, x_{27} = 3, x_{28} = 5, x_{29} = 4, x_{30} = 4, x_{31} = 6$	1
R_5	S_5	$x_0 = 2, x_2 = 6, x_3 = 5, x_4 = 8, x_5 = 6, x_7 = 8, x_8 = 12, x_9 = 14, x_{10} = 15$ $x_{11} = 12, x_{13} = 1, x_{14} = 12, x_{16} = 6, x_{17} = 12, x_{19} = 5, x_{20} = 9, x_{22} = 14$ $x_{23} = 6, x_{24} = 6, x_{27} = 8, x_{28} = 14, x_{29} = 9, x_{30} = 9, x_{31} = 6$	$\frac{1}{2^{49}}$

Table 6: The 5-round Differential of Serpent in [7]

We can easily get the following differential whose fourth-round probability is $\frac{1}{2^{13}}$ and the fifth-round probability is $\frac{1}{2^{33}}$ (table 7). So, we can improve the 5-round differential probability from $\frac{1}{2^{80}}$ to $\frac{1}{2^{67}}$.

In addition, we give some other differentials in the following:

(1) The 6-round (rounds 5-10) differential with the probability $\frac{1}{2^{97}}$ (See table 8).

R		Differences	Pr
I		$x_0 = 14$,$x_4 = 10$,$x_6 = 13$,$x_7 = 2$,$x_{18} = 12$,$x_{31} = 13$	
R_1	S_1	$x_0 = 8$,$x_4 = 4$,$x_6 = 2$,$x_7 = 10$,$x_{18} = 1$, $x_{31} = 2$	$\frac{1}{2^{13}}$
	LT	$x_4 = 5$,$x_7 = 10$	1
R_2	S_2	$x_4 = 4$,$x_7 = 10$	$\frac{1}{2^5}$
	LT	$x_{29} = 4$	1
R_3	S_3	$x_{29} = 10$	$\frac{1}{2^3}$
	LT	$x_3 = 1$,$x_4 = 8$,$x_9 = 1$,$x_{26} = 4$,$x_{30} = 2$	1
R_4	S_4	$x_3 = 11$,$x_4 = 12$,$x_9 = 10$,$x_{26} = 3$,$x_{30} = 3$	$\frac{1}{2^{13}}$
	LT	$x_0 = 5$,$x_4 = 7$,$x_6 = 4$,$x_9 = 5$,$x_{10} = 10$,$x_{11} = 12$,$x_{13} = 3$,$x_{14} = 12$ $x_{16} = 12$,$x_{17} = 11$,$x_{19} = 1$,$x_{21} = 8$,$x_{26} = 9$,$x_{27} = 2$,$x_{29} = 4$,$x_{31} = 3$	1
R_5	S_5	$x_0 = 14$,$x_4 = 8$,$x_6 = 11$,$x_9 = 14$,$x_{10} = 1$,$x_{11} = 4$,$x_{13} = 8$,$x_{14} = 4$ $x_{16} = 4$,$x_{17} = 1$,$x_{19} = 6$,$x_{21} = 12$,$x_{26} = 5$,$x_{27} = 13$,$x_{29} = 9$,$x_{31} = 8$	$\frac{1}{2^{33}}$

Table 7: The Improved 5-round (round 2-round 6) Differential of Serpent

In this case, if we only consider 5-round (round 6 to round 10), we can get a 5 rounds truncated differential with the probability of $\frac{1}{2^{61}}$ (Table 9).

(2) The 6 rounds (2-7) differential with the probability $\frac{1}{2^{97}}$ (table 10).

(3) The 5 rounds (3-7) differential with the probability $\frac{1}{2^{66}}$ (table 11).

5 The Possible Best Differential Analysis about Serpent

In this section, our main aim is to discuss the best differentials about some cases, in which there are active S-boxes as possible as least. According to Lemma, we can deduce the best differential probability about these cases. These differentials reflect the bound of the best differential about Serpent.

Theorem 1: If the S-boxes inputs of i-th round only has one active S-box with nonzero input difference, then one of the following two cases holds.

(1) The number of active S-boxes in i-(i+1) rounds is ≥ 8, i.e., $n_i + n_{i+1} \geq 8$.

(2) The number of the active S-boxes in i-($i+1$) round is < 8, then the number n_{i+2} of active S-boxes in the ($i+2$)-round must be $> 12 - n_i - n_{i+1}$, where n_k denotes the active S-boxes number in the k-th round.

Proof: Our proof is based on table 12 to table 16. Table 12 to table 16 list all the possible cases which have the minimal active S-boxes in ($i+2$)-th

R		Differences	Pr
I		$x_0 = 1,\ x_1 = 6,\ x_2 = 2,\ x_4 = 10,\ x_7 = 4,\ x_8 = 1$ $x_{11} = 5,\ x_{13} = 5,\ x_{16} = 1,\ x_{17} = 1,\ x_{21} = 1$ $x_{23} = 5,\ x_{24} = 4,\ x_{26} = 4,\ x_{27} = 6,\ x_{30} = 4$	
R_1	S_4	$x_0 = 10,\ x_1 = 9,\ x_2 = 6,\ x_4 = 5,\ x_7 = 3,\ x_8 = 13$ $x_{11} = 12,\ x_{13} = 12,\ x_{16} = 10,\ x_{17} = 14,\ x_{21} = 7$ $x_{23} = 12,\ x_{24} = 3,\ x_{26} = 11,\ x_{27} = 4,\ x_{30} = 3$	$\frac{1}{2^{36}}$
	LT	$x_1 = 6,\ x_5 = 12,\ x_6 = 5,\ x_7 = 13,\ x_8 = 10,\ x_{14} = 12$ $x_{16} = 5,\ x_{17} = 8,\ x_{20} = 12,\ x_{26} = 1$	1
R_2	S_5	$x_1 = 1,\ x_5 = 4,\ x_6 = 2,\ x_7 = 10,\ x_8 = 10,\ x_{14} = 2$ $x_{16} = 2,\ x_{17} = 12,\ x_{20} = 2,\ x_{26} = 3$	$\frac{1}{2^{28}}$
	LT	$x_7 = 6, x_{10} = 4, x_{14} = 12, x_{17} = 14, x_{27} = 10, x_{30} = 4$	1
R_3	S_6	$x_7 = 4, x_{10} = 10, x_{14} = 1, x_{17} = 1, x_{27} = 2, x_{30} = 10$	$\frac{1}{2^{14}}$
	LT	$x_0 = 5, x_3 = 1$	1
R_4	S_7	$x_0 = 4, x_3 = 10$	$\frac{1}{2^5}$
	LT	$x_{25} = 4$	1
R_5	S_0	$x_{25} = 10$	$\frac{1}{2^2}$
	LT	$x_0 = 8, x_5 = 1, x_{22} = 4, x_{26} = 2, x_{31} = 1$	1
R_6	S_1	$x_0 = 14, x_5 = 3, x_{22} = 6, x_{26} = 3, x_{31} = 3$	$\frac{1}{2^{13}}$

Table 8: The 6-round (5-10) Differential of Serpent

R		Differences	Pr
I		$x_1 = 11,\ x_5 = 12,\ x_6 = 6,\ x_7 = 1,\ x_8 = 1$ $x_{14} = 6,\ x_{16} = 6,\ x_{17} = 8,\ x_{20} = 6,\ x_{26} = 1$	
R_2	S_5	$x_1 = 1,\ x_5 = 4,\ x_6 = 2,\ x_7 = 10,\ x_8 = 10,\ x_{14} = 2$ $x_{16} = 2,\ x_{17} = 12,\ x_{20} = 2,\ x_{26} = 3$	$\frac{1}{2^{27}}$
	LT	$x_7 = 6, x_{10} = 4, x_{14} = 12, x_{17} = 14, x_{27} = 10, x_{30} = 4$	1
R_3	S_6	$x_7 = 4, x_{10} = 10, x_{14} = 1, x_{17} = 1, x_{27} = 2, x_{30} = 10$	$\frac{1}{2^{14}}$
	LT	$x_0 = 5, x_3 = 1$	1
R_4	S_7	$x_0 = 4, x_3 = 10$	$\frac{1}{2^5}$
	LT	$x_{25} = 4$	1
R_5	S_0	$x_{25} = 10$	$\frac{1}{2^2}$
	LT	$x_0 = 8, x_5 = 1, x_{22} = 4, x_{26} = 2, x_{31} = 1$	1
R_6	S_1	$x_0 = 14, x_5 = 3, x_{22} = 6, x_{26} = 3, x_{31} = 3$	$\frac{1}{2^{13}}$

Table 9: The 5-Round (6-10) Differential of Serpent with the Probability of $\frac{1}{2^{54}}$

R		Differences	Pr
I		$x_0 = 14$,$x_2 = 3$,$x_5 = 12$,$x_9 = 14$,$x_{13} = 9$,$x_{16} = 13$ $x_{18} = 12$,$x_{21} = 1$,$x_{22} = 13$,$x_{26} = 4$,$x_{29} = 8$,$x_{31} = 13$	
R_1	S_1	$x_0 = 8$,$x_2 = 5$,$x_5 = 11$,$x_9 = 8$,$x_{13} = 4$,$x_{16} = 2$ $x_{18} = 11$,$x_{21} = 10$,$x_{22} = 2$,$x_{26} = 12$,$x_{29} = 14$,$x_{31} = 2$	$\frac{1}{2^{25}}$
R_2	LT	$x_1 = 10$, $x_4 = 1$, $x_{16} = 10$, $x_{20} = 5$, $x_{22} = 6$, $x_{23} = 15$, $x_{27} = 5$, $x_{30} = 4$	1
	S_2	$x_1 = 4$, $x_4 = 10$, $x_{16} = 8$, $x_{20} = 4$, $x_{22} = 2$, $x_{23} = 10$, $x_{27} = 4$, $x_{30} = 10$	$\frac{1}{2^{23}}$
	LT	$x_{23} = 10$,$x_{26} = 4$	1
R_3	S_3	$x_3 = 4$,$x_{26} = 10$	$\frac{1}{2^6}$
	LT	$x_{16} = 4$	1
R_4	S_4	$x_{16} = 3$	$\frac{1}{2^2}$
	LT	$x_2 = 1$,$x_3 = 1$,$x_{14} = 4$,$x_{17} = 2$,$x_{22} = 1$,$x_{30} = 2$,	1
R_5	S_5	$x_2 = 10$,$x_3 = 6$,$x_{14} = 5$,$x_{17} = 10$,$x_{22} = 3$,$x_{30} = 10$	$\frac{1}{2^{17}}$
	LT	$x_0 = 5$,$x_1 = 1$,$x_3 = 2$,$x_4 = 5$,$x_7 = 6$,$x_9 = 8$ $x_{12} = 1$,$x_{14} = 1$,$x_{20} = 4$,$x_{23} = 2$,$x_{28} = 7$,$x_{31} = 6$	1
R_6	S_6	$x_0 = 3$,$x_1 = 14$,$x_3 = 7$,$x_4 = 3$,$x_7 = 1$,$x_9 = 11$ $x_{12} = 14$,$x_{14} = 14$,$x_{20} = 10$,$x_{23} = 7$,$x_{28} = 2$,$x_{31} = 1$	$\frac{1}{2^{24}}$

Table 10: The 6 Rounds (2-7) Differential of Serpent

R		Differences	Pr
I		$x_{12} = 3$, $x_{15} = 13$, $x_{18} = 13$, $x_{19} = 14$, $x_{21} = 4$, $x_{22} = 1$ $x_{25} = 2$, $x_{26} = 7$, $x_{27} = 3$, $x_{28} = 3$, $x_{29} = 4$	
R_1	S_0	$x_{12} = 1$, $x_{15} = 8$, $x_{18} = 8$, $x_{19} = 4$, $x_{21} = 10$, $x_{22} = 14$ $x_{25} = 12$, $x_{26} = 4$, $x_{27} = 2$, $x_{28} = 2$, $x_{29} = 10$	$\frac{1}{2^{25}}$
	LT	$x_{22} = 10$, $x_{25} = 8$, $x_{28} = 10$,	1
R_2	S_1	$x_{22} = 4$, $x_{25} = 14$, $x_{28} = 10$	$\frac{1}{2^7}$
	LT	$x_{15} = 4$,$x_{18} = 4$	1
R_3	S_2	$x_{15} = 6$,$x_{18} = 10$	$\frac{1}{2^4}$
	LT	$x_8 = 4$,$x_{13} = 4$,$x_{16} = 2$,$x_{21} = 1$	1
R_4	S_3	$x_8 = 11$,$x_{13} = 12$,$x_{16} = 10$,$x_{21} = 6$	$\frac{1}{2^{11}}$
	LT	$x_5 = 4$,$x_9 = 2$,$x_{10} = 4$,$x_{14} = 5$,$x_{15} = 8$ $x_{20} = 9$,$x_{25} = 3$,$x_{26} = 1$,$x_{30} = 1$	1
R_5	S_4	$x_5 = 3$,$x_9 = 6$,$x_{10} = 3$,$x_{14} = 12$,$x_{15} = 12$ $x_{20} = 2$,$x_{25} = 1$,$x_{26} = 7$,$x_{30} = 7$	$\frac{1}{2^{19}}$

Table 11: The 5-round (3-7) Differential of Serpent

round if the previous two rounds have the number of active S-boxes less than 8 ($n_i + n_{i+1} < 8$).

It is noted that, the S-boxes in the first row denote the S-boxes used in i-th round. By the structure of Serpent, if the S-box in i-th round is S_k, the S-box in $(i+1)$-th round is S_{k+1}. For example, the second column in table 12 implies that:

$$1 \overset{(i,S_0)}{\longrightarrow} 2 \overset{(i+1,S_1)}{\longrightarrow} 8$$

It implies such a 3-round $(i-(i+2))$ differential that, there is one active S-box in i-th round with S-box S_0, two active S-boxes in $(i+1)$-th round with S_1, and eight active S-boxes in $(i+2)$-th round with S_2. All other tables (table 13-table 27) have the similar representations.

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	1	1	1	1	1	1	1	1
$i+1$	2	2	2	2	2	2	2	2
$i+2$	≥ 8	≥ 12	≥ 12	≥ 12	≥ 8	≥ 12	≥ 11	≥ 12

Table 12: The Active S-boxes Distribution of Serpent

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	1	1	1	1	1	1	1	1
$i+1$	3	3	3	3	3	3	3	3
$i+2$	≥ 8	≥ 13	≥ 9	≥ 13	≥ 8	≥ 12	≥ 12	≥ 12

Table 13: The Active S-boxes Distribution of Serpent

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	1	1	1	1	1	1	1	1
$i+1$	4	4	4	4	4	4	4	4
$i+2$	≥ 11	≥ 17	≥ 16	≥ 14	≥ 13	≥ 15	≥ 14	≥ 17

Table 14: The Active S-boxes Distribution of Serpent

¿From lemma and the theorem 1, we know that, if there is one active S-box in i-th round, one of the following two differentials must hold: 2-round

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	1	1	1	1	1	1	1	1
$i+1$	5	5	5	5	5	5	5	5
$i+2$	≥ 17	≥ 19	≥ 18	≥ 16	≥ 17	≥ 17	≥ 17	≥ 18

Table 15: The Active S-boxes Distribution of Serpent

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	1	1	1	1	1	1	1	1
$i+1$	6	6	6	6	6	6	6	6
$i+2$	≥ 13	≥ 17	≥ 15	≥ 17	≥ 12	≥ 16	≥ 13	≥ 15

Table 16: The Active S-boxes Distribution of Serpent

(i-($i+1$)) differential holds with the probability $\leq \frac{1}{2^{16}}$, or 3-round (i-($i+2$) rounds) differential holds with the probability $\leq \frac{1}{2^{24}}$.

Theorem 2: If the S-boxes inputs of i-th round only has two active S-boxes with nonzero input differences, at least one of the three cases holds:

(1) The number of active S-boxes in i-(i+1) rounds is ≥ 8, i.e, $n_i+n_{i+1} \geq 8$.

(2) $n_i + n_{i+1} < 8$, and $n_i + n_{i+1} + n_{i+2} \geq 12$.

(3) $n_i+n_{i+1} < 8$, $n_i+n_{i+1}+n_{i+2} < 12$, and $n_i+n_{i+1}+n_{i+2}+n_{i+3} \geq 16$.

The proof is deduced from table 17 to table 22.

It is noted that, all the symbols "$\geq$" in the last rows of table 17-table 27 are omitted.

R	S_0		S_1			S_2			S_3	
i	2		2			2			2	
$i+1$	1		1			1			1	
$i+2$	6	8	5	6	8	5	6	8	6	7
$i+3$	21	20	18	16	17	16	17	17	12	14

Table 17: The Active S-boxes Distribution of Serpent

Theorem 3: If the S-boxes inputs of i-th round only has three active S-boxes with nonzero difference, at least one of the following three cases holds:

(1) The number of active S-boxes in i-(i+1) rounds is ≥ 8, i.e, $n_i+n_{i+1} \geq$

R	S_4		S_5				S_6		S_7		
i	2		2				2		2		
$i+1$	1		1				1		1		
$i+2$	6	7	5	6	7	8	6	7	5	6	7
$i+3$	18	19	17	13	12	16	19	20	17	17	15

Table 18: The Active S-boxes Distribution of Serpent

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	2	2	2	2	2	2	2	2
$i+1$	2	2	2	2	2	2	2	2
$i+2$	12	8	8	8	8	8	8	8

Table 19: The Active S-boxes Distribution of Serpent

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	2	2	2	2	2	2	2	2
$i+1$	3	3	3	3	3	3	3	3
$i+2$	9	9	11	13	10	11	11	11

Table 20: The Active S-boxes Distribution of Serpent

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	2	2	2	2	2	2	2	2
$i+1$	4	4	4	4	4	4	4	4
$i+2$	5	13	9	10	5	11	9	9
$i+3$	16				12			

Table 21: The Active S-boxes Distribution of Serpent

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	2	2	2	2	2	2	2	2
$i+1$	5	5	5	5	5	5	5	5
$i+2$	8	12	9	10	7	11	8	8

Table 22: The Active S-boxes Distribution of Serpent

8.

(2) $n_i + n_{i+1} < 8$, and $n_i + n_{i+1} + n_{i+2} \geq 12$.

(3) $n_i + n_{i+1} < 8$, $n_i + n_{i+1} + n_{i+2} < 12$, and $n_i + n_{i+1} + n_{i+2} + n_{i+3} \leq 16$.

See table 23-table 27.

R	S_0			S_1		S_2			S_3	
i	3			3		3			3	
$i+1$	1			1		1			1	
$i+2$	5	6	7	5	6	5	6	7	5	6
$i+3$	19	17	18	18	16	16	17	15	17	16

Table 23: The Active S-boxes Distribution of Serpent

R	S_4			S_5			S_6			S_7		
i	3			3			3			3		
$i+1$	1			1			1			1		
$i+2$	5	6	7	5	6	7	5	6	7	5	6	7
$i+3$	17	16	15	17	15	17	18	15	15	17	13	12

Table 24: The Active S-boxes Distribution of Serpent

R	S_0	S_1		S_2		S_3	S_4	S_5			S_6	S_7
i	3	3		3		3	3	3			3	3
$i+1$	2	2		2		2	2	2			2	2
$i+2$	6	4	6	3	4	7	6	3	4	6	6	6
$i+3$	18	9	18	13	13		14	13	11	16	19	17

Table 25: The Active S-boxes Distribution of Serpent

¿From theorem 1 to theorem 3, we get the following theorem.

Theorem 4: The best 16-round differential is not higher than $\frac{1}{2^{118}}$, and the best 17-round differential is not higher than $\frac{1}{2^{126}}$.

Our analysis result is better than the conjecture of the designers about Serpent. The designers guess that the probability of the best 28-round differential is not higher than $\frac{1}{2^{120}}$, but they didn't provide enough analysis evidence.

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	3	3	3	3	3	3	3	3
$i+1$	3	3	3	3	3	3	3	3
$i+2$	5	9	6	8	5	7	9	7
$i+3$	13				12			

Table 26: The Active S-boxes Distribution of Serpent

R	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
i	3	3	3	3	3	3	3	3
$i+1$	4	4	4	4	4	4	4	4
$i+2$	4	9	5	7	7	8	7	6
$i+3$	16							

Table 27: The Active S-boxes Distribution of Serpent

So, the resistance of Serpent against differential attacks is higher than that expected by the designers.

6 Conclusion and Discussions

In this paper, we give some differential analysis on Serpent. From these differentials, we conclude that the best 16-round differential is not higher than $\frac{1}{2^{118}}$, and the best 17-round differential is not higher than $\frac{1}{2^{126}}$. The differential estimation of the designer is conservative.

A secure encryption algorithm should resists other attacks such as impossible differential attack, linear attacks [5, 6, 11]etc. In our paper, we only consider the security strength against differential attack.

References

[1] Ross J. Anderson, Eli Biham, Lars R. Knudsen, Serpent: A Proposal for the Advanced Encryption Standard. Available at: http://www.cs.technion.ac.il/ biham/Reports/Serpent.

[2] Ross J. Anderson, Eli Biham, Lars R. Knudsen, Serpent: A New Block Cipher Proposal, Proceedings of Fast Software Encryption-FSE'98, Springer LNCS Vol.1372 pp.222-238.

[3] Eli Biham, On Matsui's Linear Cryptanalysis, Advances in Cryptology-Eurocrypto'94, 1994.

[4] Eli Biham, Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer 1993.

[5] Eli.Biham, A.Biryukov, O. Dunkelmann, E.Richardson, and A.Shamir, Cryptanalysis of Skipjack-3XOR in 2^{20} time and using 2^9 chosen plaintexts,July2,1998,http://www.cs.technion.ac.il/ biham/Reports/Skipjack/.

[6] Eli.Biham, A.Biryukov, and A.Shamir, Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials, Advances in Cryptology-Eurocrypto'99, pp 12-23, 1999, Springer-verlag, Also available at http://www.cs.technion.ac.il/ biham/Reports/Skipjack/.

[7] Don, Coppersmith, The Data Encryption Standard (DES) and its Strength Against Attacks, IBM Journal of Research and Developments, vol. 38, no. 3, pp.243-250, 1994.

[8] Orr Dunkelman, An Analysis of Serpent-p and Serpent-p-ns, presented in the second AES Conference, available at: http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm

[9] T. Kohno, J. Kelsey, B. Schneier, Preliminary Cryptanalysis of Reduced-Round Serpent, presented in the third AES candidate conference, available at: http://csrc.nist.gov/encryption/aes/round2/conf3/aes3agenda.html

[10] L.R.Knudsen, M. J. B. Robshaw, D. Wagner, Truncated Differentials and Skipjack,

[11] M. Matsui, Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology-Eurocrypt'93, Springer LNCS, Vol. 765, pp. 368-397.

A Appendix

S-boxes	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_0:	3	8	15	1	10	6	5	11	14	13	4	2	7	0	9	12
S_1:	15	12	2	7	9	0	5	10	1	11	14	8	6	13	3	4
S_2:	8	6	7	9	3	12	10	15	13	1	14	4	0	11	5	2
S_3:	0	15	11	8	12	9	6	3	13	1	2	4	10	7	5	14
S_4:	1	15	8	3	12	0	11	6	2	5	4	10	9	14	7	13
S_5:	15	5	2	11	4	10	9	12	0	3	14	8	13	6	7	1
S_6:	7	2	12	5	8	4	6	11	14	9	1	15	13	3	10	0
S_7:	1	13	15	0	14	8	2	11	7	4	12	10	9	3	5	6

Table 28: The S-boxes in Serpent-1 and Serpent-p-ns

Inpit	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x16	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	2	0	2	2	2	0	0	0	2	2	0	4	0
2_x	0	0	0	0	0	0	0	0	0	2	2	0	4	2	2	4
3_x	0	2	2	2	0	0	0	2	0	4	0	2	2	0	0	0
4_x	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4	0
5_x	0	0	2	0	4	2	0	0	2	0	2	2	0	0	2	0
6_x	0	2	2	4	0	2	2	4	0	0	0	0	0	0	0	0
7_x	0	0	2	0	4	2	0	0	2	2	0	2	0	2	0	0
8_x	0	0	0	2	0	2	2	2	0	0	0	2	2	4	0	0
9_x	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0
A_x	0	2	2	2	0	0	0	2	0	0	4	2	2	0	0	0
B_x	0	2	2	0	0	2	2	0	0	0	0	0	4	0	0	4
C_x	0	2	0	0	4	0	2	0	2	2	0	2	0	2	0	0
D_x	0	0	0	4	0	0	0	4	4	0	0	0	0	0	0	4
E_x	0	2	0	0	4	0	2	0	2	0	2	2	0	0	2	0
F_x	0	2	2	0	0	2	2	0	4	0	0	0	0	0	0	4

Table 29: The XORs difference distribution of S0-box

Inpit	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	2	0	2	2	2	0	2	2	2	0	0	0	2
2_x	0	0	0	2	0	2	0	0	0	2	2	2	2	2	0	2
3_x	0	0	2	2	0	4	0	0	2	2	0	0	0	0	4	0
4_x	0	0	0	0	0	0	4	4	0	0	0	0	4	4	0	0
5_x	0	0	2	0	0	2	0	0	2	0	2	2	2	2	0	2
6_x	0	0	2	0	0	2	2	2	2	0	2	2	0	0	0	2
7_x	0	0	2	2	0	4	0	0	2	2	0	0	0	0	4	0
8_x	0	0	0	0	0	0	2	2	0	0	0	0	2	2	4	4
9_x	0	2	0	0	4	0	2	0	0	4	2	0	0	2	0	0
A_x	0	2	0	4	4	0	0	2	0	0	2	0	2	0	0	0
B_x	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
C_x	0	4	2	2	0	0	0	0	2	2	0	4	0	0	0	0
D_x	0	2	4	0	4	0	2	0	0	0	2	0	0	2	0	0
E_x	0	2	0	0	4	0	0	2	4	0	2	0	2	0	0	0
F_x	0	4	0	0	0	0	0	0	0	0	0	4	0	0	4	4

Table 30: The XORs difference distribution of S1-box

Inpit	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	0	0	2	0	2	0	0	2	2	2	0	4	2
2_x	0	0	0	4	0	4	0	0	0	4	0	0	0	0	0	4
3_x	0	4	2	0	0	0	2	0	0	2	0	0	2	0	2	2
4_x	0	0	0	0	0	0	4	0	0	0	4	4	0	4	0	0
5_x	0	4	0	2	2	2	2	0	2	0	0	0	2	0	0	0
6_x	0	0	2	2	2	2	0	0	2	2	0	0	0	0	2	2
7_x	0	0	0	0	4	2	0	2	0	0	2	2	2	0	0	2
8_x	0	0	0	2	0	2	0	4	0	2	0	0	0	4	0	2
9_x	0	0	0	2	0	0	0	2	4	2	2	2	2	0	0	0
A_x	0	0	2	0	2	0	4	0	2	0	4	0	0	0	2	0
B_x	0	4	0	0	2	0	2	0	2	2	0	0	2	0	0	2
C_x	0	0	2	0	2	0	0	0	2	0	0	4	0	4	2	0
D_x	0	4	2	2	0	2	2	0	0	0	0	0	2	0	2	0
E_x	0	0	2	0	2	0	0	4	2	0	0	0	0	4	2	0
F_x	0	0	4	2	0	0	0	2	0	2	2	2	2	0	0	0

Table 31: The XORs difference distribution of S2-box

Inpit	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	2	0	4	2	0	0	0	0	2	2	2	0	2
2_x	0	0	0	0	0	2	0	2	0	2	4	2	0	0	0	4
3_x	0	0	2	2	4	0	0	0	2	2	0	0	0	0	0	4
4_x	0	0	0	0	0	0	4	4	0	0	2	2	2	2	0	0
5_x	0	2	0	2	0	0	0	0	2	2	2	2	2	0	2	0
6_x	0	2	0	2	0	0	2	2	4	0	0	0	2	0	0	2
7_x	0	0	2	4	4	2	0	0	0	2	0	0	0	0	2	0
8_x	0	0	0	2	0	0	2	0	0	2	0	0	2	4	4	0
9_x	0	2	2	2	0	0	2	0	2	0	2	2	0	0	0	2
A_0	0	0	2	0	2	0	2	2	0	4	0	2	2	0	0	0
B_x	0	2	2	0	2	2	0	0	0	2	2	0	2	2	0	0
C_x	0	2	0	0	2	0	2	2	4	0	2	0	0	0	2	0
D_x	0	2	2	0	2	4	0	2	0	0	0	0	0	4	0	0
E_x	0	4	2	0	0	2	0	0	0	0	0	2	0	2	2	2
F_x	0	0	2	0	0	0	0	2	2	0	2	2	2	0	4	0

Table 32: The XORs difference distribution of S3-box

Inpit	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	0	0	0	0	4	0	0	2	2	2	2	4	0
2_x	0	0	0	2	0	0	4	2	0	2	0	0	2	0	2	2
3_x	0	2	2	0	2	0	0	2	2	2	2	2	0	0	0	0
4_x	0	0	0	4	0	2	0	2	0	0	0	4	0	2	0	2
5_x	0	2	0	2	0	0	0	0	2	2	0	0	4	2	2	0
6_x	0	0	0	2	4	2	0	0	2	2	2	0	0	2	0	0
7_x	0	0	2	2	2	0	0	2	2	0	2	0	0	0	0	4
8_x	0	0	0	2	0	2	0	0	0	2	2	2	4	0	2	0
9_x	0	2	4	0	2	0	2	2	0	2	0	0	0	2	0	0
A_0	0	0	2	0	0	4	2	0	2	0	2	2	0	2	0	0
B_x	0	4	0	0	0	2	0	2	0	0	0	4	0	2	0	2
C_x	0	2	0	0	0	2	0	0	2	0	0	0	2	0	4	4
D_x	0	2	4	0	2	2	2	0	0	2	0	0	0	0	0	2
E_x	0	2	2	2	0	0	2	0	2	2	2	0	0	2	0	0
F_x	0	0	0	0	4	0	4	0	2	0	2	0	2	0	2	0

Table 33: The XORs difference distribution of S4-box

Inpit	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	2	0	2	4	0	0	2	2	2	0	0	2	0
2_x	0	0	0	0	0	0	2	2	0	0	2	2	0	4	4	0
3_x	0	2	0	2	2	0	0	2	4	0	0	0	2	2	0	0
4_x	0	0	0	0	0	2	0	2	0	4	0	4	0	2	0	2
$5-x$	0	2	2	0	0	2	2	0	0	0	0	0	0	0	4	4
6_x	0	2	2	2	0	0	4	2	0	2	0	0	0	0	2	0
7_x	0	2	0	2	2	2	0	0	4	0	0	0	2	0	0	2
8_x	0	0	0	2	0	0	2	0	0	2	0	0	4	2	2	2
9_x	0	0	2	0	0	4	0	2	2	0	2	2	2	0	0	0
A_x	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0	0
B_x	0	4	0	0	0	2	0	2	0	0	0	4	0	2	0	2
C_x	0	0	2	2	4	2	0	2	0	2	2	0	0	0	0	0
D_x	0	2	2	2	0	0	0	2	2	2	2	0	2	0	0	0
E_x	0	0	2	0	2	0	0	0	2	2	2	0	0	2	0	4
F_x	0	0	2	0	4	0	2	0	0	0	2	0	4	0	2	0

Table 34: The XORs difference distribution of S5-box

Inpit	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	0	0	2	0	2	0	2	2	0	2	2	4	0
2_x	0	0	0	2	0	0	2	4	0	0	0	2	0	0	2	4
3_x	0	2	4	2	0	0	0	0	2	2	0	0	0	2	2	0
4_x	0	0	0	2	0	0	2	0	0	0	4	2	0	0	2	4
5_x	0	2	0	4	2	2	0	2	0	0	2	0	0	2	0	0
6_x	0	4	0	0	4	0	0	0	0	4	0	0	4	0	0	0
7_x	0	0	4	2	2	0	0	0	2	0	0	0	2	2	2	0
8_x	0	0	0	0	0	2	0	2	0	2	2	4	2	2	0	0
9_x	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
A_x	0	0	4	0	2	0	2	0	2	0	0	2	2	2	0	0
B_x	0	0	0	2	0	4	2	0	4	0	0	2	0	0	2	0
C_x	0	2	0	0	2	2	4	2	0	0	2	0	0	2	0	0
D_x	0	2	0	0	2	0	0	0	0	2	4	0	2	0	0	4
E_x	0	2	4	0	0	0	2	0	2	2	0	2	0	2	0	0
F_x	0	0	0	0	0	4	0	4	4	0	0	0	0	0	0	4

Table 35: The XORs difference distribution of S6-box

Inpit	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	0	4	0	0	2	2	0	2	0	0	2
2_x	0	0	0	2	0	2	0	0	0	0	0	2	4	2	4	0
3_x	0	2	2	0	0	2	2	0	2	0	2	0	0	2	0	2
4_x	0	0	0	0	0	2	0	2	0	2	0	2	2	2	2	2
5_x	0	0	2	2	4	0	0	0	0	2	2	0	0	2	0	2
6_x	0	2	4	2	0	2	2	0	2	2	0	0	0	0	0	0
7_x	0	4	0	2	0	0	0	2	0	0	2	0	0	0	2	4
8_x	0	0	0	2	0	0	2	4	0	2	2	2	0	2	0	0
9_0	0	2	0	0	2	4	0	0	0	0	2	0	2	2	2	0
A_x	0	0	0	0	2	0	0	2	4	0	0	4	0	2	2	0
B_x	0	4	2	0	0	0	0	2	2	0	0	4	0	2	0	0
C_x	0	2	0	0	0	0	2	0	2	2	2	0	2	0	4	0
D_x	0	0	2	0	2	2	0	2	2	2	2	0	0	0	0	2
E_x	0	0	4	2	2	2	2	0	0	0	0	2	0	0	0	2
F_x	0	0	0	0	4	0	2	2	2	2	0	0	4	0	0	0

Table 36: The XORs difference distribution of S7-box