程序验证

设置剪枝条件：P2<464（64\*7+16）

故，当且仅当：

情况一：

1. 只有1个活跃S盒
2. 差分传播概率为16
3. 输入查分为001000、000100、001100中的一种（4,8,12）

情况二：

8个S盒都不活跃

以下为程序运行结果：

aj=1

count=8

index=0,DDT\_SearchInOrderX=52

index=1,DDT\_SearchInOrderX=0

count=7

**aj=2**

count=8

index=0,**DDT\_SearchInOrderX=8**

aj=3

count=8

aj=4

count=8

aj=5

count=8

aj=6

count=8

aj=7

count=8

aj=8

**(64.000000,16.000000,64.000000,64.000000,64.000000,64.000000,64.000000,64.000000)**

count=8

index=1,DDT\_SearchInOrderX=29

index=2,DDT\_SearchInOrderX=54

index=3,DDT\_SearchInOrderX=59

index=4,DDT\_SearchInOrderX=61

index=5,DDT\_SearchInOrderX=0

count=7

aj=3

count=8

index=0,DDT\_SearchInOrderX=32

index=1,DDT\_SearchInOrderX=39

index=2,DDT\_SearchInOrderX=45

index=3,DDT\_SearchInOrderX=52

index=4,DDT\_SearchInOrderX=0

count=7

aj=4

count=8

index=0,DDT\_SearchInOrderX=1

aj=5

count=8

aj=6

index=1,DDT\_SearchInOrderX=1

aj=5

count=8

aj=6

index=2,DDT\_SearchInOrderX=1

aj=5

count=8

aj=6

index=3,DDT\_SearchInOrderX=1

aj=5

count=8

aj=6

index=4,DDT\_SearchInOrderX=7

aj=5

count=8

aj=6

index=5,DDT\_SearchInOrderX=17

index=6,DDT\_SearchInOrderX=17

index=7,DDT\_SearchInOrderX=20

index=8,DDT\_SearchInOrderX=23

index=9,DDT\_SearchInOrderX=25

index=10,DDT\_SearchInOrderX=29

index=11,DDT\_SearchInOrderX=40

index=12,DDT\_SearchInOrderX=42

index=13,DDT\_SearchInOrderX=42

index=14,DDT\_SearchInOrderX=43

index=15,DDT\_SearchInOrderX=46

index=16,DDT\_SearchInOrderX=46

index=17,DDT\_SearchInOrderX=46

index=18,DDT\_SearchInOrderX=46

index=19,DDT\_SearchInOrderX=47

index=20,DDT\_SearchInOrderX=47

index=21,DDT\_SearchInOrderX=47

index=22,DDT\_SearchInOrderX=47

index=23,DDT\_SearchInOrderX=50

index=24,DDT\_SearchInOrderX=54

index=25,DDT\_SearchInOrderX=56

index=26,DDT\_SearchInOrderX=59

index=27,DDT\_SearchInOrderX=59

index=28,DDT\_SearchInOrderX=63

index=29,DDT\_SearchInOrderX=0

count=7

aj=5

count=8

index=0,DDT\_SearchInOrderX=5

aj=6

count=8

aj=7

index=1,DDT\_SearchInOrderX=13

aj=6

count=8

aj=7

index=2,DDT\_SearchInOrderX=26

index=3,DDT\_SearchInOrderX=53

index=4,DDT\_SearchInOrderX=0

count=7

**aj=6**

count=8

index=0,DDT\_SearchInOrderX=1

aj=7

count=8

aj=8

index=1,**DDT\_SearchInOrderX=8**

aj=7

count=8

aj=8

**(64.000000,64.000000,64.000000,64.000000,64.000000,16.000000,64.000000,64.000000)**

count=8

index=2,DDT\_SearchInOrderX=34

index=3,DDT\_SearchInOrderX=60

index=4,DDT\_SearchInOrderX=0

count=7

aj=7

count=8

index=0,DDT\_SearchInOrderX=24

index=1,DDT\_SearchInOrderX=37

index=2,DDT\_SearchInOrderX=43

index=3,DDT\_SearchInOrderX=51

index=4,DDT\_SearchInOrderX=52

index=5,DDT\_SearchInOrderX=54

index=6,DDT\_SearchInOrderX=57

index=7,DDT\_SearchInOrderX=58

index=8,DDT\_SearchInOrderX=0

count=7

aj=8

**(64.000000,64.000000,64.000000,64.000000,64.000000,64.000000,64.000000,64.000000)**

count=8

index=0,DDT\_SearchInOrderX=1

index=1,DDT\_SearchInOrderX=10

index=2,DDT\_SearchInOrderX=20

index=3,DDT\_SearchInOrderX=26

index=4,DDT\_SearchInOrderX=31

index=5,DDT\_SearchInOrderX=32

index=6,DDT\_SearchInOrderX=0

count=7

请按任意键继续. . .