### Shadow-32：

#### 等效S盒差分均匀度：

64

#### 差分均匀度对应等效S盒差分特征：

输入差分:

00000001

输出差分，概率:

00000000 , 2^-2

00000010 , 2^-2

10000000 , 2^-2

10000010 , 2^-2

输入差分:

00000010

输出差分，概率:

00000000 , 2^-2

00000001 , 2^-2

00000100 , 2^-2

00000101 , 2^-2

输入差分:

00000100

输出差分，概率:

00000000 , 2^-2

00000010 , 2^-2

00001000 , 2^-2

00001010 , 2^-2

输入差分:

00001000

输出差分，概率:

00000000 , 2^-2

00000100 , 2^-2

00010000 , 2^-2

00010100 , 2^-2

输入差分:

00010000

输出差分，概率:

00000000 , 2^-2

00001000 , 2^-2

00100000 , 2^-2

00101000 , 2^-2

输入差分:

00100000

输出差分，概率:

00000000 , 2^-2

00010000 , 2^-2

01000000 , 2^-2

01010000 , 2^-2

输入差分:

01000000

输出差分，概率:

00000000 , 2^-2

00100000 , 2^-2

10000000 , 2^-2

10100000 , 2^-2

输入差分:

10000000

输出差分，概率:

00000000 , 2^-2

00000001 , 2^-2

01000000 , 2^-2

01000001 , 2^-2

### Shadow-64：

#### 等效S盒差分均匀度：

16384

#### 差分均匀度对应等效S盒差分特征：

输入差分:

0000000000000001

输出差分，概率:

0000000000000000 , 2^-2

0000000000000010 , 2^-2

0000000010000000 , 2^-2

0000000010000010 , 2^-2

输入差分:

0000000000000010

输出差分，概率:

0000000000000000 , 2^-2

0000000000000100 , 2^-2

0000000100000000 , 2^-2

0000000100000100 , 2^-2

输入差分:

0000000000000100

输出差分，概率:

0000000000000000 , 2^-2

0000000000001000 , 2^-2

0000001000000000 , 2^-2

0000001000001000 , 2^-2

输入差分:

0000000000001000

输出差分，概率:

0000000000000000 , 2^-2

0000000000010000 , 2^-2

0000010000000000 , 2^-2

0000010000010000 , 2^-2

输入差分:

0000000000010000

输出差分，概率:

0000000000000000 , 2^-2

0000000000100000 , 2^-2

0000100000000000 , 2^-2

0000100000100000 , 2^-2

输入差分:

0000000000100000

输出差分，概率:

0000000000000000 , 2^-2

0000000001000000 , 2^-2

0001000000000000 , 2^-2

0001000001000000 , 2^-2

输入差分:

0000000001000000

输出差分，概率:

0000000000000000 , 2^-2

0000000010000000 , 2^-2

0010000000000000 , 2^-2

0010000010000000 , 2^-2

输入差分:

0000000010000000

输出差分，概率:

0000000000000000 , 2^-2

0000000100000000 , 2^-2

0100000000000000 , 2^-2

0100000100000000 , 2^-2

输入差分:

0000000100000000

输出差分，概率:

0000000000000000 , 2^-2

0000001000000000 , 2^-2

1000000000000000 , 2^-2

1000001000000000 , 2^-2

输入差分:

0000001000000000

输出差分，概率:

0000000000000000 , 2^-2

0000000000000001 , 2^-2

0000010000000000 , 2^-2

0000010000000001 , 2^-2

输入差分:

0000010000000000

输出差分，概率:

0000000000000000 , 2^-2

0000000000000010 , 2^-2

0000100000000000 , 2^-2

0000100000000010 , 2^-2

输入差分:

0000100000000000

输出差分，概率:

0000000000000000 , 2^-2

0000000000000100 , 2^-2

0001000000000000 , 2^-2

0001000000000100 , 2^-2

输入差分:

0001000000000000

输出差分，概率:

0000000000000000 , 2^-2

0000000000001000 , 2^-2

0010000000000000 , 2^-2

0010000000001000 , 2^-2

输入差分:

0010000000000000

输出差分，概率:

0000000000000000 , 2^-2

0000000000010000 , 2^-2

0100000000000000 , 2^-2

0100000000010000 , 2^-2

输入差分:

0100000000000000

输出差分，概率:

0000000000000000 , 2^-2

0000000000100000 , 2^-2

1000000000000000 , 2^-2

1000000000100000 , 2^-2

输入差分:

1000000000000000

输出差分，概率:

0000000000000000 , 2^-2

0000000000000001 , 2^-2

0000000001000000 , 2^-2

0000000001000001 , 2^-2