CSEC 508: Applied Cryptanalysis
Homework 2

GENC, ECE BEREN

1.

S_0:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0xc	0x5	0x6	0xb	0x9	0x0	0xa	0xd	0x3	0xe	0xf	0x8	0x4	0x7	0x1	0x2

S_0^{-1}:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x5	0xe	0xf	0x8	0xc	0x1	0x2	0xd	0xb	0x4	0x6	0x3	0x0	0x7	0x9	0xa

S_1:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0xe	0x4	0xd	0x1	0x2	0xf	0xb	0x8	0x3	0xa	0x6	0xc	0x5	0x9	0x0	0x7

S_1^{-1}:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0xe	0x3	0x4	0x8	0x1	0xc	0xa	0xf	0x7	0xd	0x9	0x6	0xb	0x2	0x0	0x5

S_2:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	0xb	0xc	0x5	0x6	0x1	0x9	0xa	0x3	0xf	0xe	0x8	0xd	0x4	0x2	0x7

S_2^{-1}:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	0x5	0xe	0x8	0xd	0x3	0x4	0xf	0xb	0x6	0x7	0x1	0x2	0xc	0xa	0x9

(Code for getting inverse S-boxes:

```
S_boxes = [list("c56b90ad3ef84712"),
           list("e4d12fb83a6c5907"),
           list("0bc5619a3fe8d427")]

def reverseSBox(sbox):
    inverseSbox = [0] * 16  # Initialize an empty inverse S-box

    for i, value in enumerate(sbox):
        inverseSbox[int(value, 16)] = hex(i)[2:].upper().zfill(2)

    return inverseSbox

def obtaining_inverse_SBoxes(SBoxes):
    inverseSBoxes = [reverseSBox(sbox) for sbox in SBoxes]
    return inverseSBoxes

inverse_SBoxes = obtaining_inverse_SBoxes(S_boxes)

# Print the inverse S-boxes in the desired format
for i, inverse_SBox in enumerate(inverse_SBoxes):
    print(f"Inverse S-box {i}: {', '.join(inverse_SBox)}")
```

Output:

Inverse S-box 0: 05, 0E, 0F, 08, 0C, 01, 02, 0D, 0B, 04, 06, 03, 00, 07, 09, 0A

Inverse S-box 1: 0E, 03, 04, 08, 01, 0C, 0A, 0F, 07, 0D, 09, 06, 0B, 02, 00, 05

Inverse S-box 2: 00, 05, 0E, 08, 0D, 03, 04, 0F, 0B, 06, 07, 01, 02, 0C, 0A, 09)

2.

DDT TABLE of S_0:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0xc	0x5	0x6	0xb	0x9	0x0	0xa	0xd	0x3	0xe	0xf	0x8	0x4	0x7	0x1	0x2

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
A	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
B	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
C	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
D	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

Differential Uniformity of S_0: 4

DDT TABLE S_1:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0xe	0x4	0xd	0x1	0x2	0xf	0xb	0x8	0x3	0xa	0x6	0xc	0x5	0x9	0x0	0x7

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Differential Uniformity of S_1: 8

DDT TABLE S_2:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	0xb	0xc	0x5	0x6	0x1	0x9	0xa	0x3	0xf	0xe	0x8	0xd	0x4	0x2	0x7

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	2	2	2	0	4	0	2	2	0	0	0
2	0	0	0	2	0	0	0	2	0	0	0	2	2	2	2	4
3	0	2	0	0	0	2	2	2	2	0	2	2	2	0	0	0
4	0	0	0	0	0	2	2	0	0	0	2	2	2	0	2	4
5	0	2	2	0	0	0	2	2	0	2	2	0	2	2	0	0
6	0	4	0	2	2	0	0	0	2	2	2	0	2	0	0	0
7	0	0	2	2	2	2	0	0	0	0	4	0	0	4	0	0
8	0	0	2	2	2	2	0	0	0	0	0	4	0	4	0	0
9	0	0	2	0	2	0	0	0	4	0	0	2	2	0	2	2
A	0	0	0	2	4	0	2	0	0	0	2	0	0	0	4	2
B	0	2	0	4	0	2	2	2	2	0	0	0	0	2	0	0
C	0	0	4	0	0	2	0	2	0	0	0	0	0	2	4	2
D	0	2	2	0	4	0	2	2	0	2	0	2	0	0	0	0
E	0	4	2	0	0	2	0	0	2	2	2	0	2	0	0	0
F	0	0	0	0	0	0	2	2	4	4	0	0	0	0	2	2

Differential Uniformity of S_2: 4

3.

DDT TABLE S_0^{-1}:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x5	0xe	0xf	0x8	0xc	0x1	0x2	0xd	0xb	0x4	0x6	0x3	0x0	0x7	0x9	0xa

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	2	0	4	0	0	0	2	0	2	0	4
2	0	0	0	0	0	0	2	2	0	2	2	0	2	4	2	0
3	0	4	2	2	0	0	0	0	2	0	2	0	0	2	2	0
4	0	0	0	2	0	2	0	0	0	4	0	2	0	2	0	4
5	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0
6	0	0	2	4	2	0	2	2	0	2	0	0	0	0	2	0
7	0	4	0	2	2	0	0	0	2	0	0	0	2	2	2	0
8	0	0	0	0	0	0	2	2	0	2	2	4	2	0	2	0
9	0	4	0	0	2	2	0	0	2	0	0	2	2	0	2	0
A	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0
B	0	0	0	2	0	2	4	0	4	0	0	2	0	2	0	0
C	0	0	2	0	2	4	2	2	0	2	0	0	0	0	2	0
D	0	4	2	0	0	2	0	0	2	0	2	2	0	0	2	0
E	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
F	0	0	0	0	0	0	4	4	4	0	0	0	0	0	0	4

Differential Uniformity of S_0^{-1}: 4

DDT TABLE S_1^{-1}:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0xe	0x3	0x4	0x8	0x1	0xc	0xa	0xf	0x7	0xd	0x9	0x6	0xb	0x2	0x0	0x5

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	4	0	0	0	2	2	0	2	4	0	2
2	0	0	0	2	0	0	0	2	0	0	2	8	0	0	2	0
3	0	2	2	0	2	0	4	2	0	0	0	0	0	0	4	0
4	0	0	0	2	0	0	0	2	0	2	0	0	2	0	2	6
5	0	0	6	0	0	2	4	0	0	0	0	2	2	0	0	0
6	0	0	2	0	6	2	0	2	2	0	0	0	2	0	0	0
7	0	2	2	0	0	0	0	0	2	4	0	2	0	4	0	0
8	0	0	0	0	0	0	0	0	0	2	6	0	0	2	6	0
9	0	2	2	4	2	0	0	2	0	0	0	0	0	0	0	4
A	0	4	0	2	0	4	0	2	0	2	0	0	0	2	0	0
B	0	0	0	0	4	0	0	0	4	2	2	0	2	0	0	2
C	0	4	0	2	2	2	2	0	0	2	0	0	0	2	0	0
D	0	2	0	0	0	0	2	0	4	0	0	2	6	0	0	0
E	0	0	2	0	0	0	2	0	2	0	4	0	0	2	2	2
F	0	0	0	4	0	2	2	4	2	0	0	2	0	0	0	0

Differential Uniformity of S_1^{-1}: 8

DDT TABLE S_2^{-1}:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	0x5	0xe	0x8	0xd	0x3	0x4	0xf	0xb	0x6	0x7	0x1	0x2	0xc	0xa	0x9

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	2	4	0	0	0	0	2	0	2	4	0
2	0	0	0	0	0	2	0	2	2	2	0	0	4	2	2	0
3	0	2	2	0	0	0	2	2	2	0	2	4	0	0	0	0
4	0	0	0	0	0	0	2	2	2	2	4	0	0	4	0	0
5	0	2	0	2	2	0	0	2	2	0	0	2	2	0	2	0
6	0	2	0	2	2	2	0	0	0	0	2	2	0	2	0	2
7	0	2	2	2	0	2	0	0	0	0	0	2	2	2	0	2
8	0	0	0	2	0	0	2	0	0	4	0	2	0	0	2	4
9	0	4	0	0	0	2	2	0	0	0	0	0	0	2	2	4
A	0	0	0	2	2	2	2	4	0	0	2	0	0	0	2	0
B	0	2	2	2	2	0	0	0	4	2	0	0	0	2	0	0
C	0	2	2	2	2	2	2	0	0	2	0	0	0	0	2	0
D	0	0	2	0	0	2	0	4	4	0	0	2	2	0	0	0
E	0	0	2	0	2	0	0	0	0	2	4	0	4	0	0	2
F	0	0	4	0	4	0	0	0	0	2	2	0	2	0	0	2

Differential Uniformity of S_2^{-1}: 4

The relationship between the S^i and S_i^{-1} in terms of differential uniformity is that their differential uniformity values are the same. S-box performs substitution, and it is one of the main components of symmetric key algorithms. It determines how resistant algorithm against the attacks. Inverse S-box is reverse of S-box, and it is used for decryption. It maps output values of the S-box back to input values. Therefore, switching input and output values of S-box does not change differential uniformity values of S-box. Therefore, S^i and S_i^{-1} has the same differential uniformity values.

4. Undisturbed bits of S_0, S_1 and S_2's S-boxes:

S-box	Input difference	Output difference	Output difference	Input difference
S_0	0001	???1	0001	???1
S_0	1000	???1	0100	???1
S_0	1001	???0	0101	???0

S_1	-	-	0010	??1?
S_1	-	-	1000	1???
S_1	-	-	1010	???1
S_2	-	-	-	-

(Instead of writing code, pen and paper method was used.)

5. Differential factors of S-boxes:

Cipher	S-box	Differential Factors
S_0	**S[x]:** 0xc, 0x5, 0x6, 0xb, 0x9, 0x0, 0xa, 0xd, 0x3, 0xe, 0xf, 0x8, 0x4, 0x7, 0x1, 0x2	$\lambda = 1 \quad \mu = 5$ $\lambda = F \quad \mu = F$
S_1	**S[x]:** 0xe, 0x4, 0xd, 0x1, 0x2, 0xf, 0xb, 0x8, 0x3, 0xa, 0x6, 0xc, 0x5, 0x9, 0x0, 0x7	-
S_2	**S[x]:** 0x0, 0xb, 0xc, 0x5, 0x6, 0x1, 0x9, 0xa, 0x3, 0xf, 0xe, 0x8, 0xd, 0x4, 0x2, 0x7	-

(Code for obtaining differential factors of S-boxes:

```
def find_differential_factors(s_box, output_diff):
    differential_factors = []
    for lambda_val in range(16):
        invariant = True
        for x in range(16):
            for y in range(16):
                if s_box[x] ^ s_box[y] == output_diff:
                    if s_box[x ^ lambda_val] ^ s_box[y ^ lambda_val] !=
output_diff:
                        invariant = False
                        break
            if not invariant:
                break
        if invariant:
            differential_factors.append(lambda_val)
    return differential_factors


S_boxes = [
```

```
    [0xC, 0x5, 0x6, 0xB, 0x9, 0x0, 0xA, 0xD, 0x3, 0xE, 0xF, 0x8, 0x4,
0x7, 0x1, 0x2],
    [0xE, 0x4, 0xD, 0x1, 0x2, 0xF, 0xB, 0x8, 0x3, 0xA, 0x6, 0xC, 0x5,
0x9, 0x0, 0x7],
    [0x0, 0xB, 0xC, 0x5, 0x6, 0x1, 0x9, 0xA, 0x3, 0xF, 0xE, 0x8, 0xD,
0x4, 0x2, 0x7]
]

output_diff_values = range(1, 16)  # Exclude output difference of 0

for i, s_box in enumerate(S_boxes):
    print(f"*** S-Box {i+1} ***")
    for output_diff in output_diff_values:
        differential_factors = find_differential_factors(s_box,
output_diff)
        print(f"Differential Factors λ = {differential_factors}, Output
Difference μ = {output_diff}")
    print()
```

Output:

*** S-Box 1 ***

Differential Factors λ = [0], Output Difference μ = 1

Differential Factors λ = [0], Output Difference μ = 2

Differential Factors λ = [0], Output Difference μ = 3

Differential Factors λ = [0], Output Difference μ = 4

Differential Factors λ = [0, 1], Output Difference μ = 5

Differential Factors λ = [0], Output Difference μ = 6

Differential Factors λ = [0], Output Difference μ = 7

Differential Factors λ = [0], Output Difference μ = 8

Differential Factors λ = [0], Output Difference μ = 9

Differential Factors λ = [0], Output Difference μ = 10

Differential Factors λ = [0], Output Difference μ = 11

Differential Factors λ = [0], Output Difference μ = 12

Differential Factors λ = [0], Output Difference μ = 13

Differential Factors λ = [0], Output Difference μ = 14

Differential Factors λ = [0, 15], Output Difference μ = 15

*** S-Box 2 ***

Differential Factors λ = [0], Output Difference μ = 1

Differential Factors λ = [0], Output Difference μ = 2

Differential Factors λ = [0], Output Difference μ = 3

Differential Factors λ = [0], Output Difference μ = 4

Differential Factors λ = [0], Output Difference μ = 5

Differential Factors λ = [0], Output Difference μ = 6

Differential Factors λ = [0], Output Difference μ = 7

Differential Factors λ = [0], Output Difference μ = 8

Differential Factors λ = [0], Output Difference μ = 9

Differential Factors λ = [0], Output Difference μ = 10

Differential Factors λ = [0], Output Difference μ = 11

Differential Factors λ = [0], Output Difference μ = 12

Differential Factors λ = [0], Output Difference μ = 13

Differential Factors λ = [0], Output Difference μ = 14

Differential Factors λ = [0], Output Difference μ = 15

*** S-Box 3 ***

Differential Factors λ = [0], Output Difference μ = 1

Differential Factors λ = [0], Output Difference μ = 2

Differential Factors λ = [0], Output Difference μ = 3

Differential Factors λ = [0], Output Difference μ = 4

Differential Factors λ = [0], Output Difference μ = 5

Differential Factors λ = [0], Output Difference μ = 6

Differential Factors λ = [0], Output Difference μ = 7

Differential Factors λ = [0], Output Difference μ = 8

Differential Factors λ = [0], Output Difference μ = 9

Differential Factors λ = [0], Output Difference μ = 10

Differential Factors λ = [0], Output Difference μ = 11

Differential Factors λ = [0], Output Difference μ = 12

Differential Factors λ = [0], Output Difference μ = 13

Differential Factors λ = [0], Output Difference μ = 14

Differential Factors λ = [0], Output Difference μ = 15)

6. Differential factors of inverse S-boxes:

Cipher	S-box	Differential Factors
S_0^{-1}	**S[x]:** 0x5, 0xe, 0xf, 0x8, 0xc, 0x1, 0x2, 0xd, 0xb, 0x4, 0x6, 0x3, 0x0, 0x7, 0x9, 0xa	λ =5 μ = 1 λ =F μ = F
S_1^{-1}	**S[x]:** 0xe, 0x3, 0x4, 0x8, 0x1, 0xc, 0xa, 0xf, 0x7, 0xd, 0x9, 0x6, 0xb, 0x2, 0x0, 0x5	-
S_2^{-1}	**S[x]:** 0x0, 0x5, 0xe, 0x8, 0xd, 0x3, 0x4, 0xf, 0xb, 0x6, 0x7, 0x1, 0x2, 0xc, 0xa, 0x9	-

For S-box and inverse S-box, the relationship between λ and μ values has specific pattern. For S-box λ =1, μ =5 and for inverse S-box λ =5 and μ = 1. As a result, if S-box has differential factor λ and output difference μ, inverse S-box has differential factor μ and output difference λ.

(Code for obtaining differential factors of inverse S-boxes:

```
def find_differential_factors(s_box, output_diff):
    differential_factors = []
    for lambda_val in range(16):
        invariant = True
        for x in range(16):
            for y in range(16):
                if s_box[x] ^ s_box[y] == output_diff:
                    if s_box[x ^ lambda_val] ^ s_box[y ^ lambda_val] !=
output_diff:
                        invariant = False
                        break
            if not invariant:
                break
        if invariant:
            differential_factors.append(lambda_val)
    return differential_factors
```

```
S_boxes = [
    [0x5, 0xe, 0xf, 0x8, 0xc, 0x1, 0x2, 0xd, 0xb, 0x4, 0x6, 0x3, 0x0,
0x7, 0x9, 0xa],
    [0xe, 0x3, 0x4, 0x8, 0x1, 0xc, 0xa, 0xf, 0x7, 0xd, 0x9, 0x6, 0xb,
0x2, 0x0, 0x5],
    [0x0, 0x5, 0xe, 0x8, 0xd, 0x3, 0x4, 0xf, 0xb, 0x6, 0x7, 0x1, 0x2,
0xc, 0xa, 0x9]
]

output_diff_values = range(1, 16)  # Exclude output difference of 0

for i, s_box in enumerate(S_boxes):
    print(f"*** Inverse S-Box {i+1} ***")
    for output_diff in output_diff_values:
        differential_factors = find_differential_factors(s_box,
output_diff)
        print(f"Differential Factors λ = {differential_factors}, Output
Difference μ = {output_diff}")
    print()
```

Output:

*** Inverse S-Box 1 ***

Differential Factors λ = [0, 5], Output Difference μ = 1

Differential Factors λ = [0], Output Difference μ = 2

Differential Factors λ = [0], Output Difference μ = 3

Differential Factors λ = [0], Output Difference μ = 4

Differential Factors λ = [0], Output Difference μ = 5

Differential Factors λ = [0], Output Difference μ = 6

Differential Factors λ = [0], Output Difference μ = 7

Differential Factors λ = [0], Output Difference μ = 8

Differential Factors λ = [0], Output Difference μ = 9

Differential Factors λ = [0], Output Difference μ = 10

Differential Factors λ = [0], Output Difference μ = 11

Differential Factors λ = [0], Output Difference μ = 12

Differential Factors λ = [0], Output Difference μ = 13

Differential Factors λ = [0], Output Difference μ = 14

Differential Factors λ = [0, 15], Output Difference μ = 15

*** Inverse S-Box 2 ***

Differential Factors λ = [0], Output Difference μ = 1

Differential Factors λ = [0], Output Difference μ = 2

Differential Factors λ = [0], Output Difference μ = 3

Differential Factors λ = [0], Output Difference μ = 4

Differential Factors λ = [0], Output Difference μ = 5

Differential Factors λ = [0], Output Difference μ = 6

Differential Factors λ = [0], Output Difference μ = 7

Differential Factors λ = [0], Output Difference μ = 8

Differential Factors λ = [0], Output Difference μ = 9

Differential Factors λ = [0], Output Difference μ = 10

Differential Factors λ = [0], Output Difference μ = 11

Differential Factors λ = [0], Output Difference μ = 12

Differential Factors λ = [0], Output Difference μ = 13

Differential Factors λ = [0], Output Difference μ = 14

Differential Factors λ = [0], Output Difference μ = 15

*** Inverse S-Box 3 ***

Differential Factors λ = [0], Output Difference μ = 1

Differential Factors λ = [0], Output Difference μ = 2

Differential Factors λ = [0], Output Difference μ = 3

Differential Factors λ = [0], Output Difference μ = 4

Differential Factors λ = [0], Output Difference μ = 5

Differential Factors λ = [0], Output Difference μ = 6

Differential Factors λ = [0], Output Difference μ = 7

Differential Factors λ = [0], Output Difference μ = 8

Differential Factors λ = [0], Output Difference μ = 9

Differential Factors λ = [0], Output Difference μ = 10

Differential Factors λ = [0], Output Difference μ = 11

Differential Factors λ = [0], Output Difference μ = 12

Differential Factors λ = [0], Output Difference μ = 13

Differential Factors λ = [0], Output Difference μ = 14

Differential Factors λ = [0], Output Difference μ = 15)

7.

LAT TABLE S_0:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0xc	0x5	0x6	0xb	0x9	0x0	0xa	0xd	0x3	0xe	0xf	0x8	0x4	0x7	0x1	0x2

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	-4	0	-4	0	0	0	0	0	-4	0	4
2	0	0	2	2	-2	-2	0	0	2	-2	0	4	0	4	-2	2
3	0	0	2	2	2	-2	-4	0	-2	2	-4	0	0	0	-2	-2
4	0	0	-2	2	-2	-2	0	4	-2	-2	0	-4	0	0	-2	2
5	0	0	-2	2	-2	2	0	0	2	2	-4	0	4	0	2	2
6	0	0	0	-4	0	0	-4	0	0	-4	0	0	4	0	0	0
7	0	0	0	4	4	0	0	0	0	-4	0	0	0	0	4	0
8	0	0	2	-2	0	0	-2	2	-2	2	0	0	-2	2	4	4
9	0	4	-2	-2	0	0	2	-2	-2	-2	-4	0	-2	2	0	0
A	0	0	4	0	2	2	2	-2	0	0	0	-4	2	2	-2	2
B	0	-4	0	0	-2	-2	2	-2	-4	0	0	0	2	2	2	-2
C	0	0	0	0	-2	-2	-2	-2	4	0	0	-4	-2	2	2	-2
D	0	4	4	0	-2	-2	2	2	0	0	0	0	2	-2	2	-2
E	0	0	2	2	-4	4	-2	-2	-2	-2	0	0	-2	-2	0	0
F	0	4	-2	2	0	0	-2	-2	-2	2	4	0	2	2	0	0

Linear Uniformity of S_0: 4

LAT TABLE S_1:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0xe	0x4	0xd	0x1	0x2	0xf	0xb	0x8	0x3	0xa	0x6	0xc	0x5	0x9	0x0	0x7

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	-2	-2	0	0	-2	6	2	2	0	0	2	2	0	0
2	0	0	-2	-2	0	0	-2	-2	0	0	2	2	0	0	-6	2
3	0	0	0	0	0	0	0	0	2	-6	-2	-2	2	2	-2	-2
4	0	2	0	-2	-2	-4	-2	0	0	-2	0	2	2	-4	2	0
5	0	-2	-2	0	-2	0	4	2	-2	0	-4	2	0	-2	-2	0
6	0	2	-2	4	2	0	0	2	0	-2	2	4	-2	0	0	-2
7	0	-2	0	2	2	-4	2	0	-2	0	2	0	4	2	0	2
8	0	0	0	0	0	0	0	0	-2	2	2	-2	2	-2	-2	-6
9	0	0	-2	-2	0	0	-2	-2	-4	0	-2	2	0	4	2	-2
A	0	4	-2	2	-4	0	2	-2	2	2	0	0	2	2	0	0
B	0	4	0	-4	4	0	4	0	0	0	0	0	0	0	0	0
C	0	-2	4	-2	-2	0	2	0	2	0	2	4	0	2	0	-2
D	0	2	2	0	-2	4	0	2	-4	-2	2	0	2	0	0	2
E	0	2	2	0	-2	-4	0	2	-2	0	0	-2	-4	2	-2	0
F	0	-2	-4	-2	-2	0	2	0	0	-2	4	-2	-2	0	2	0

Linear Uniformity of S_1: 6

LAT TABLE S_2:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	0xb	0xc	0x5	0x6	0x1	0x9	0xa	0x3	0xf	0xe	0x8	0xd	0x4	0x2	0x7

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	0	-2	0	-2	0	2	0	2	-4	2	4	2	0	2
2	0	-2	0	2	0	-2	0	2	2	4	2	0	2	-4	2	0
3	0	0	0	0	0	4	0	4	2	-2	-2	2	-2	-2	2	2
4	0	0	0	4	0	0	0	4	-2	-2	2	-2	2	2	-2	2
5	0	2	0	2	0	-2	0	-2	2	-4	2	4	2	0	2	0
6	0	-2	-4	2	4	2	0	-2	0	2	0	2	0	2	0	2
7	0	0	4	0	4	0	0	0	4	0	0	0	0	0	-4	0
8	0	0	2	-2	2	-2	0	0	0	0	2	-2	-2	2	4	4
9	0	2	2	4	-2	0	4	-2	0	2	-2	0	-2	0	0	2
A	0	2	-2	0	2	0	4	2	2	0	0	-2	0	2	2	-4
B	0	4	-2	-2	-2	2	0	0	2	2	4	0	0	0	-2	2
C	0	0	2	2	-2	2	-4	0	2	2	0	0	0	4	2	-2
D	0	2	2	0	2	4	0	-2	-2	0	0	-2	4	-2	2	0
E	0	2	2	0	2	0	0	2	-4	2	2	4	-2	0	0	-2
F	0	-4	2	-2	-2	2	4	0	0	0	2	2	2	2	0	0

Linear Uniformity of S_2: 4

8.

LAT TABLE S_0^{-1}:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x5	0xe	0xf	0x8	0xc	0x1	0x2	0xd	0xb	0x4	0x6	0x3	0x0	0x7	0x9	0xa

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	4	0	-4	0	4	0	4
2	0	0	2	2	-2	-2	0	0	2	-2	4	0	0	4	2	-2
3	0	0	2	2	2	2	-4	4	-2	-2	0	0	0	0	2	2
4	0	0	-2	2	-2	-2	0	4	0	0	2	-2	-2	-2	-4	0
5	0	-4	-2	-2	-2	2	0	0	0	0	2	-2	-2	-2	4	0
6	0	0	0	-4	0	0	-4	0	-2	2	2	2	-2	2	-2	-2
7	0	-4	0	0	4	0	0	0	2	-2	-2	-2	-2	2	-2	-2
8	0	0	2	-2	-2	2	0	0	-2	-2	0	-4	4	0	-2	-2
9	0	0	-2	2	-2	2	-4	-4	2	-2	0	0	0	0	-2	2
A	0	0	0	-4	0	-4	0	0	0	-4	0	0	0	0	0	4
B	0	0	4	0	-4	0	0	0	0	0	-4	0	-4	0	0	0
C	0	0	0	0	0	4	4	0	-2	-2	2	2	-2	2	-2	2
D	0	-4	4	0	0	0	0	0	2	2	2	2	2	-2	-2	2
E	0	0	-2	-2	-2	2	0	4	4	0	-2	2	2	2	0	0
F	0	4	2	-2	2	2	0	0	4	0	2	-2	-2	-2	0	0

Linear Uniformity of S_0^{-1}: 4

LAT TABLE S_1^{-1}:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0xe	0x3	0x4	0x8	0x1	0xc	0xa	0xf	0x7	0xd	0x9	0x6	0xb	0x2	0x0	0x5

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	2	-2	2	-2	0	0	4	4	-2	2	2	-2
2	0	-2	-2	0	0	-2	-2	0	0	-2	-2	0	4	2	2	-4
3	0	-2	-2	0	-2	0	4	2	0	-2	2	-4	-2	0	0	-2
4	0	0	0	0	-2	-2	2	2	0	0	-4	4	-2	-2	-2	-2
5	0	0	0	0	-4	0	0	-4	0	0	0	0	0	4	-4	0
6	0	-2	-2	0	-2	4	0	2	0	-2	2	4	2	0	0	2
7	0	6	-2	0	0	2	2	0	0	-2	-2	0	0	2	2	0
8	0	2	0	2	0	-2	0	-2	-2	-4	2	0	2	-4	-2	0
9	0	2	0	-6	-2	0	-2	0	2	0	2	0	0	-2	0	-2
A	0	0	2	-2	0	-4	2	2	2	-2	0	0	2	2	0	4
B	0	0	2	-2	2	2	4	0	-2	2	0	0	4	0	-2	-2
C	0	2	0	2	2	0	-2	4	2	0	2	0	0	2	-4	-2
D	0	2	0	2	-4	-2	0	2	-2	4	2	0	2	0	2	0
E	0	0	-6	-2	2	-2	0	0	-2	2	0	0	0	0	-2	2
F	0	0	2	-2	0	0	-2	2	-6	-2	0	0	-2	2	0	0

Linear Uniformity of S_1^{-1}: 6

LAT TABLE S_2^{-1}:

0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	0x5	0xe	0x8	0xd	0x3	0x4	0xf	0xb	0x6	0x7	0x1	0x2	0xc	0xa	0x9

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	-2	0	0	2	-2	0	0	2	2	4	0	2	2	-4
2	0	0	0	0	0	0	-4	4	2	2	-2	-2	2	2	2	2
3	0	-2	2	0	4	2	2	0	-2	4	0	-2	2	0	0	-2
4	0	0	0	0	0	0	4	4	2	-2	2	-2	-2	2	2	-2
5	0	-2	-2	4	0	-2	2	0	-2	0	0	2	2	4	0	2
6	0	0	0	0	0	0	0	0	0	4	4	0	-4	0	0	4
7	0	2	2	4	4	-2	-2	0	0	-2	2	0	0	-2	2	0
8	0	0	2	2	-2	2	0	4	0	0	2	2	2	-2	-4	0
9	0	2	4	-2	-2	-4	2	0	0	2	0	2	2	0	2	0
A	0	-4	2	-2	2	2	0	0	2	-2	0	4	0	0	2	2
B	0	2	0	2	-2	4	2	0	-2	0	-2	0	0	-2	4	2
C	0	4	2	-2	2	2	0	0	-2	-2	0	0	0	4	-2	2
D	0	2	-4	-2	2	0	2	0	2	0	2	0	4	-2	0	2
E	0	0	2	2	-2	2	0	-4	4	0	2	-2	2	2	0	0
F	0	2	0	2	2	0	2	0	4	2	-4	2	-2	0	-2	0

Linear Uniformity of S_2^{-1}: 4

In terms of linear uniformity, there is a relationship between S_i and S_i^{-1}. They have same linear uniformity and non-linear measure. However, it may differ according to S-box design, but in this case they have same linear uniformity values.