Cryptography Quiz 8

Consider the SPN where the following S-box is used:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| *πS*(*z*) | E | 2 | 1 | 3 | D | 9 | 0 | 6 | F | 4 | 5 | A | 8 | C | 7 | B |

Following table has been created for the given S-box with input sum B and output sum 6 with seven missing entries which are denoted by a, b, c, d, e, f, g:

|  |  |  |  |
| --- | --- | --- | --- |
| *X* | *Y* | *X*1*⊕ X*3*⊕ X*4 | *Y*2*⊕ Y*3 |
| 0000 | 1110 | 0 | 0 |
| 0001 | 0010 | 1 | 1 |
| 0010 | 0001 | a | 0 |
| 0011 | 0011 | 0 | b |
| 0100 | 1101 | c | 1 |
| 0101 | 1001 | 1 | d |
| 0110 | 0000 | 1 | 0 |
| 0111 | 0110 | 0 | 0 |
| 1000 | 1111 | 1 | 0 |
| 1001 | 0100 | 0 | 1 |
| 1010 | 0101 | 0 | 1 |
| 1011 | 1010 | 1 | 1 |
| 1100 | 1000 | 1 | 0 |
| 1101 | 1100 | 0 | e |
| 1110 | 0111 | f | 0 |
| 1111 | 1011 | 1 | g |

1. (14 points) Find the values of a, b, c, d, e, f, g in the above table. (2 points each)

Ans.

def xor(nums: int) -> int:

    xor\_result = nums[0]

    for i in range(1, len(nums)):

        xor\_result = xor\_result ^ nums[i]

    return xor\_result

a = [0, 1, 0]

b = [0, 1]

c = [0, 0, 0]

d = [0, 0]

e = [1, 0]

f = [1, 1, 0]

g = [0, 1]

print(f"a: {xor(a)} b: {xor(b)} c: {xor(c)} d: {xor(d)} e: {xor(e)} f: {xor(f)} g: {xor(g)}")

****

1. (2 points) Compute *NL*(*B,*6) and (*B,*6).
2. (2 points) Compute (*B,*6).

Ans.

X = [0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1]

Y = [0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1]

T = []

for i in range(len(X)):

    r = X[i] ^ Y[i]

    if r == 1:

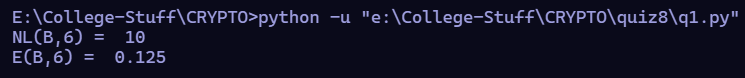
        T.append(r)

nl = len(T)

print("NL(B,6) = ", nl)

E = (nl-8)/16

print("E(B,6) = ", E)



1. (2 points) Can this pair be used to construct linear approximation?

Ans. Yes