**개요**

모든 6비트 양의 정수 x에 대해, S4(x)와 S4(x^001100)이 2비트 이상 다른지 확인하기

**함수 작성(python)**

# Python 3.4

def s\_index(x):

'''

Input 6비트 양의 정수 x < 64

Output (y, z) : y < 4, z < 16

S-box 안의 index를 계산하는 함수

'''

assert type(x) == int;

assert 0 <= x < 64;

return ((x // 32) \* 2 + x % 2, (x // 2) % 16)

# DES의 S4-Box

s4\_list = [

[7, 13, 14, 3, 0, 6, 9, 10, 1, 2, 8, 5, 11, 12, 4, 15],

[13, 8, 11, 5, 6, 15, 0, 3, 4, 7, 2, 12, 1, 10, 14, 9],

[10, 6, 9, 0, 12, 11, 7, 13, 15, 1, 3, 14, 5, 2, 8, 4],

[3, 15, 0, 6, 10, 1, 13, 8, 9, 4, 5, 11, 12, 7, 2, 14]]

def S4(x):

'''

Input 6비트 양의 정수 x < 64

Output 4비트 양의 정수

정수에 대응되는 S-box 출력값을 계산하는 함수

'''

i, j = s\_index(x);

return s4\_list[i][j]

# main contents

print(min([bin(S4(i) ^ (S4(i ^ 0b001100))).count('1') for i in range(64)]))

**실행결과**

2

**결론**

S4-박스는 위의 DES 설계원칙을 만족한다!