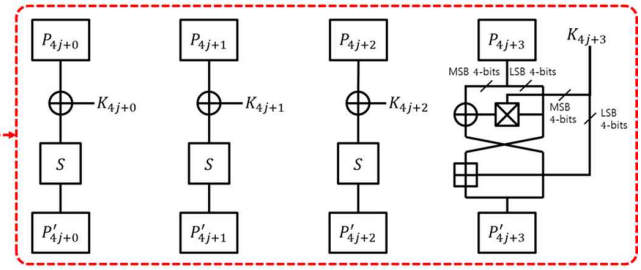
2022 암호분석경진대회

5번 문제

A는 자신의 일기를 암호화 하고자 AES의 내부함수들을 활용하여 새로운 암호를 설계하였고 일기를 암호화하는 과정에서의 전력소모량(10,000번의 단일블록 암호화 연산)이 친구 B에게 노출되었다. 하지만 전력소모량 외에 평문과 암호문의 정보는 다행히 누출되지 않았다. 친구 B는 암호가 동작하는 장비에서 펌웨어를 추출하여 역공학을 수행하였고, 그 결과 A가 설계한 암호구조를 다음과 같이 복구할 수 있었다.

```
Secret Cryptographic Algorithm
Input : PT[0…15], MK[0…15]
Output : CT[0…15]
For i:=0 to 3
    For j:=0 to 3
        PT[4j…4j+3] = F(PT[4j…4j+3], MK[4j…4j+3])
    End
    PT[0…15] = ShiftRow(PT[0…15])
    PT[0…15] = MixColumn(PT[0…15])
End
CT[0…15]:=PT[0…15]
```



[문제]

역공학을 통해 복구된 암호구조와 수집된 전력파형을 이용해 마스터키 16바이트를 찾으시오.

[참고]

1) 누출된 전력 소비 파형은 6,100개의 시점을 가진 10,000개의 파형으로 구성되어져 있으며 파일의 경로와 데이터 포맷은 다음과 같다.
   - 파일경로 : 전력파형 파일경로
   - 데이터포맷
     (4 Byte, unsigned int) : 파형 개수 N, (4 Byte, unsigned int) : 파형 길이 L,
     (8 Byte * L, Double) : 파형1, ….. , (8 Byte * L, Double) : 파형N

2) 암호 내부 연산
   - S, ShiftRow, MixColumn : AES Sbox, ShiftRow, MixColumn
   - $\oplus$, $\boxtimes$, $\boxplus$: 4-bit XOR, 곱셈연산(mod 16), 덧셈연산(mod 16)

3) 참고문헌:
   1. Linge, Yanis, Cécile Dumas, and Sophie Lambert-Lacroix. "Using the joint distributions of a cryptographic function in side channel analysis." COSADE 2014.
   2. Clavier, Christophe, and Léo Reynaud. "Improved blind side-channel analysis by exploitation of joint distributions of leakages." CHES 2017.

4) 암호키 확인용 평문, 암호문쌍

```
Plaintext  : 29622772780EF40273BAE889B7D5F579
Ciphertext : DDCDC6ECE7ED425E2651145BA7AF74AD
```

5) 평가 참고사항
   - 마스터키 복구 여부
   - 분석 기법의 신규성, 효율성 등에 대한 정성적 평가