Side Channel Analysis Contest 2022			
1. AES-128			
학교	국민대학교	이름	이현호

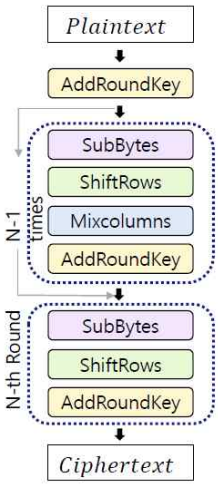
1. 블록 암호 AES-128의 특징

본 라이트업에서 사용할 기호와 그에 대한 정의는 다음 [표 1] 과 같다.

기호	정의
$X[i]$	평문 X의 i번째 바이트, $(0 \leq i < 16)$
S	AES S-Box함수

[표 1] 기호 및 정의

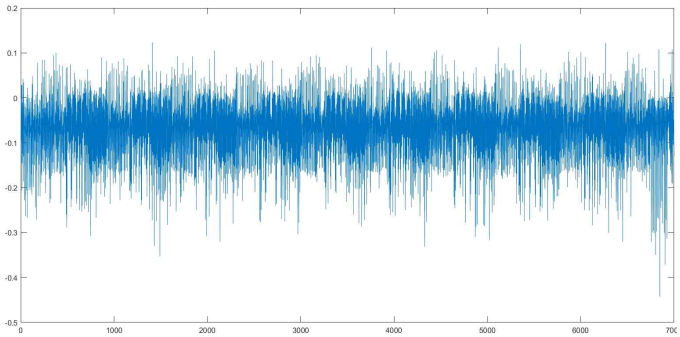
AES-128의 암호화 과정은 [그림 1] 과 같다 $(N = 10)$



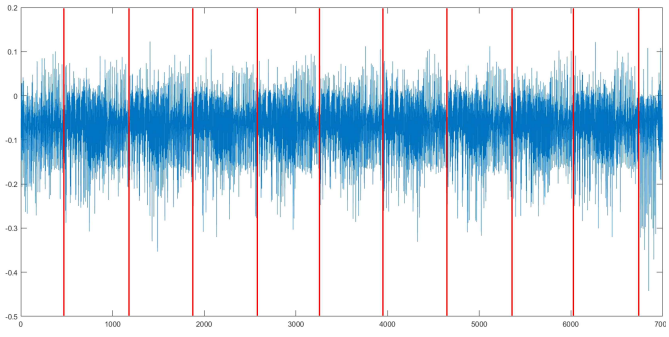
[그림 1]

AES-128의 첫 AddRoundKey 구간에서는 마스터 키가 사용된다. 따라서 주어진 전력파형 정보가 암호화 과정 중 첫 번째로 나타나는 AddRoundKey, SbuBytes, ShiftRows, Mixcolumns 함수라면 라운드 키로부터 마스터 키를 복구하는 과정 없이 마스터 키를 바로 구할 수 있다.

2. AES-128 전력파형 분석



[그림 2] AES-128 파형



[그림 3] 구간을 나눈 AES-128의 파형

[그림 2]는 주어진 AES-128의 파형[그림 3] 은 [그림 2]의 파형에서 반복적으로 보이는 패턴을 구간을 나눈 것이다. 약 11개의 구간으로 나누어지는 것을 볼 수 있다. 만약 8비트 단위로 AES-128을 구현했다면 10번 이상 반복적인 패턴이 나타날 가능성이 있는 연산 구간은 AddRoundKey와 SubBytes(S-Box 사용) 연산 구간이다.

따라서 Correlation Power Analysis(상관전력분석)에서 주어진 파형을 AddRoundKey 또는 SubBytes(S-Box 사용) 연산 구간으로 추측하고 중간값으로 AddRoundKey 또는 SubBytes(S-Box 사용) 연산을 잡는다. 사용전력모델은 8비트 Hamming Weight 모델이다.

본 답안에서는 비선형 연산인 SubBytes(S-Box함수) 구간을 중간값으로 잡고 1바이트씩 총 16번 Correlation Power Analysis를 시도하였다.

$$\text{중간값} = S[X[i] \oplus GuessKey]\,(0 \le i < 16,\ 0 \le GuessKey < 256)$$

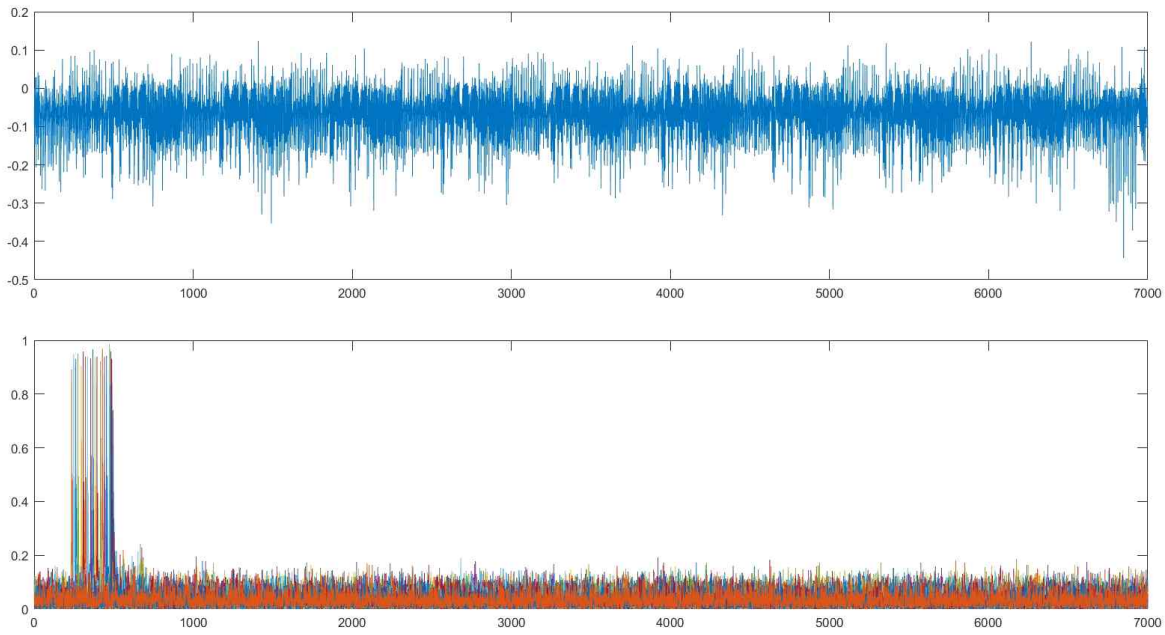
3. AES-128 마스터 키 복구

[표 2]는 $\text{중간값} = S[X[i] \oplus GuessKey]\,(0 \le i < 16,\ 0 \le GuessKey < 256)$ 으로 마스터 키에 대한 상관전력분석 실험 결과이며, 결과 중 비율은 분석 결과 가장 큰 상관계수를 두 번째로 큰 상관계수로 나눈 값을 의미한다. 분석에서 모든 비율이 3.0을 넘어 옳은 마스터 키라고 판단할 수 있다.

[그림 4]는 AES-128 전력파형의 point 위치에 따른 [표 2]의 추측 키들의 상관계수 분포를 나타낸 것이다.

분석 바이트	추측 키	상관계수	비율
1	0x47	0.890050	3.785813
2	0x4F	0.965520	3.988841
3	0x30	0.956038	4.046536
4	0x64	0.921026	3.445443
5	0x4C	0.949800	3.697554
6	0x75	0.957168	3.937621
7	0x63	0.965892	3.618273
8	0x6B	0.968551	3.050876
9	0x40	0.929102	3.815740
10	0x53	0.938613	3.761790
11	0x63	0.936402	3.367364
12	0x41	0.938012	4.149075
13	0x2D	0.949817	3.360915
14	0x43	0.984588	4.015691
15	0x54	0.939106	3.675123
16	0x46	0.940721	4.017292

[표 2] 상관전력분석 실험 결과



[그림 4] 전력파형과 추측키의 위치 관계

4. 위의 추측키를 바탕으로 복구한 Flag 의 ASCII 코드는 다음과 같다.

GOOdLuck@ScA-CTF