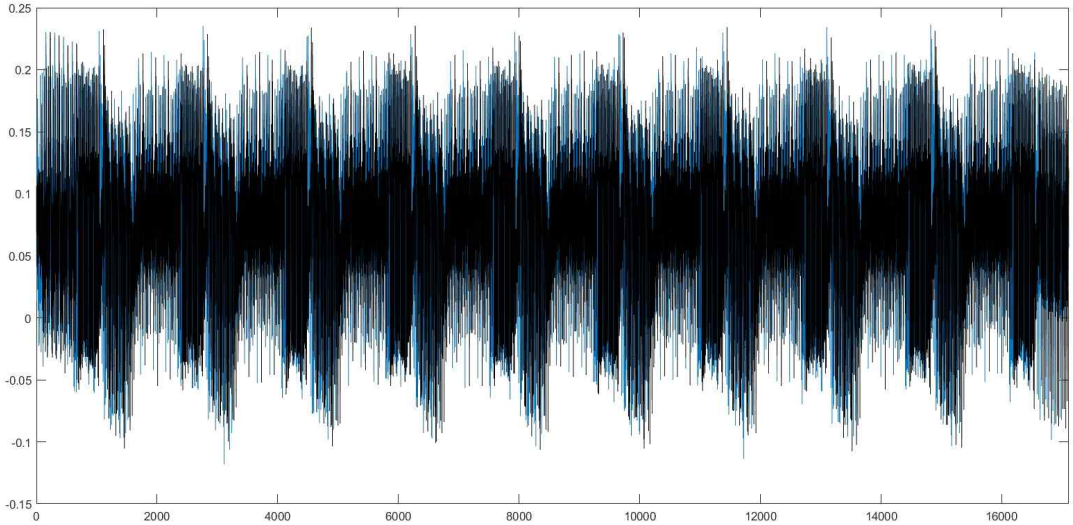
| Side Channel Analysis Contest 2022 | | | |
|---|---|---|---|
| 2. AES-128 alignment | | | |
| 학교 | 국민대학교 | 이름 | 이현호 |

## 1. 주어진 AES-128 파형의 특징

AES-128 암호화 과정의 소비 전력 신호는 기존 암호화 과정의 신호에 비해 기준 점으로부터 랜덤으로 50pt 내외로 흔들려있다. [그림 1]은 500개의 파형 중 2개의 파형을 겹쳐서 나타낸 것이다.




[그림 1] 2개의 파형을 겹쳐 나타낸 그림

## 2. 파형 정렬

상관전력분석은 각 파형에서 특정 연산의 전력값 집합과 중간값 집합과의 상관계수를 비교하여 키를 추정하는 방법이다. 만약 파형들이 흔들린다면 특정 연산과 전혀 상관없는 원소들이 포함된 집합이 될 수 있다. 따라서 다음과 같은 전략을 통해 파형들을 정렬해준다.

1) 한 개의 파형을 기준으로 특정 구간을 기준으로 다른 파형과의 구간 상관계수를 구한다.
2) 가장 높은 상관계수를 갖는 구간을 기준으로 기준 파형을 제외한 나머지 파형들의 포인트 위치를 이동시킨다.

본 라이트업에서는 CTF-2-AES-ALIGN-trace.bin 파일에서 16번째 바이트부터 나오는 4바이트 파형 정보를 포함하는 것을 첫 번째 파형으로 두었다. 정렬할때 첫 번째 파형의 200~650포인트 구간을 기준점으로 잡았다. 이를 기준으로 다음 10개 파형에 대해 분석한 결과는 [표 1] 같다.

| 파형 순서 | 포인트 구간 | 상관계수 |
|---|---|---|
| 1 | 273 ~ 723 | 0.993703 |
| 2 | 211 ~ 661 | 0.994198 |
| 3 | 200 ~ 650 | 0.995537 |
| 4 | 203 ~ 653 | 0.994792 |
| 5 | 204 ~ 654 | 0.995188 |
| 6 | 211 ~ 661 | 0.995868 |
| 7 | 255 ~ 705 | 0.995273 |
| 8 | 203 ~ 653 | 0.993699 |
| 9 | 215 ~ 665 | 0.995987 |
| 10 | 215 ~ 665 | 0.993435 |

[표 1] 가장 높은 상관계수를 갖는 구간

이 외의 나머지 489개의 파형에서 상관계수가 0.9 이상인 구간을 발견할 수 있었다.

## 3. AES-128 마스터 키 복구

본 라이트업에서 사용할 기호와 그에 대한 정의는 다음 [표 2] 과 같다.

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

[표 2] 기호 및 정의

[표 1]의 결과를 이용하여 499개의 파형을 한 파형을 기준으로 정렬시켰다.
[표 3]는 정렬 시킨 파형들을 이용하여 1라운드 S-Box연산을 중간값으로 두었을 때 실험 결과이다.
즉, $중간값 = S[X[i] \oplus GuessKey]\,(0 \leq i < 16, 0 \leq GuessKey < 256)$으로 마스터 키에 대한 상관전력분석 실험 결과이다. 결과 중 비율은 분석 결과 가장 큰 상관계수를 두 번째로 큰 상관계수로 나눈 값을 의미한다. 분석에서 모든 비율이 1.8을 넘어 옳은 마스터 키라고 판단할 수 있다.

| 분석 바이트 | 추측 키 | 상관계수 | 비율 |
|---|---|---|---|
| 1 | 0x75 | 0.681603 | 2.503141 |
| 2 | 0x43 | 0.600587 | 2.456808 |
| 3 | 0x61 | 0.681908 | 2.527143 |
| 4 | 0x6E | 0.722225 | 2.764683 |
| 5 | 0x44 | 0.464136 | 1.860471 |
| 6 | 0x6F | 0.698161 | 2.486215 |
| 7 | 0x49 | 0.725047 | 2.458917 |
| 8 | 0x74 | 0.758537 | 3.206963 |
| 9 | 0x40 | 0.529714 | 2.202735 |
| 10 | 0x73 | 0.625471 | 2.371928 |
| 11 | 0x43 | 0.790201 | 2.984207 |
| 12 | 0x61 | 0.777010 | 2.897843 |
| 13 | 0x5F | 0.645249 | 2.356901 |
| 14 | 0x63 | 0.725928 | 2.597044 |
| 15 | 0x74 | 0.738077 | 2.793030 |
| 16 | 0x66 | 0.765929 | 2.560539 |

[표 3] 파형 정렬 후 상관전력분석 실험

## 4. [표 3]의 추측 키를 바탕으로 복구한 Flag의 ASCII 코드는 다음과 같다.

uCanDoItsCa_ctf