2021 국민대학교 정보보안암호수학과 암호분석경진대회

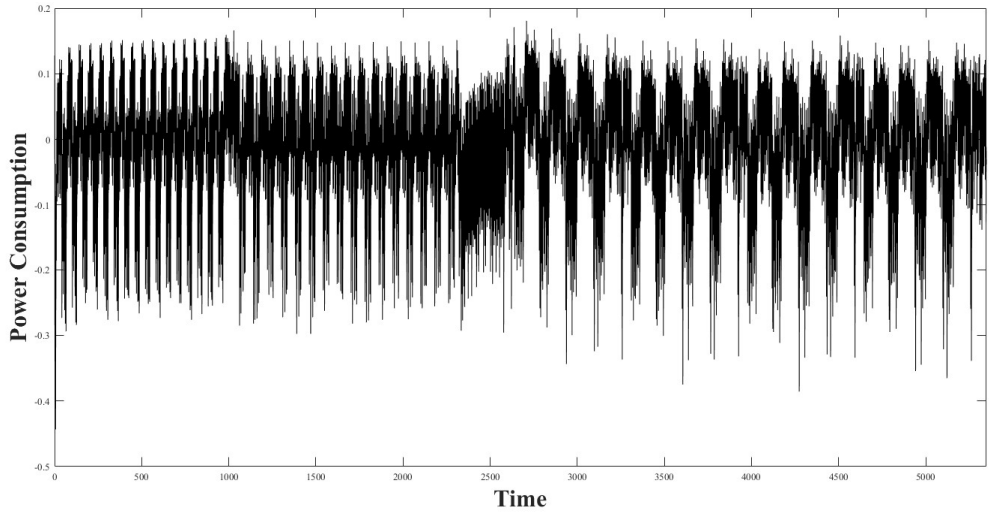
4번 문제 - 부채널 분석 (출제: 동아리 PEPSI)

부채널 분석이란, 디바이스에서 암호화 알고리즘이 동작할 때 발생하는 소리, 소비전력, 전자파와 같은 부채널 정보를 활용하여 비밀정보(비밀키)를 알아내는 분석법이다. 1999년 P.Kocher 등에 의해 제안된 Differential Power Analysis(DPA)를 시작으로, 소비전력 파형과 비밀정보 사이의 상관관계를 이용한 Correlation Power Analysis(CPA) 등 다양한 부채널 분석 기법이 연구되었다. 최근에는 인공신경망을 활용하여 기존의 부채널 분석 기법보다 적은 수의 파형으로 비밀 정보를 분석하는 MLSCA(Machine Learning Side Channel Analysis)가 주목받고 있다.

[4 - 1 문제 (10점)]

다음 그림은 AES-128 한 라운드 동작 시 발생하는 소비전력 파형이다. 주어진 파형에 Simple Power Analysis(SPA)를 적용하여 각 함수 (AddRoundKey, SubBytes, ShiftRows, MixColumns)의 연산 위치를 표시하고, 그 이유를 논리적으로 서술하라.

Hint: 제시된 파형에서 사용된 AES-128은 8-bit단위로 연산이 진행되며, SubBytes 연산의 경우 S-Box 룩업 테이블(Lookup Table)을 사용하여 구현되었다.



[4 - 2 문제 (20점)]

AES는 한 라운드키의 모든 바이트를 알면 마스터키를 복구할 수 있는 특징을 가진다. AES-128의 3번째 라운드키가 다음과 같이 주어졌을 때, AES-128 마스터키를 복구하는 코드를 구현하고, 마스터키를 복구하라.

[3라운드키]

0x32, 0x43, 0xf6, 0xa8, 0x88, 0x5a, 0x30, 0x8d, 0x31, 0x31, 0x98, 0xa2, 0xe0, 0x37, 0x07, 0x34

1번째 바이트는 0x32이며 16번째 바이트는 0x34이다. 답안에는 3라운드키를 사용한 마스터키 복구 논리와 복구한 마스터키, 복구할 때 사용된 코드를 제출해야 한다.

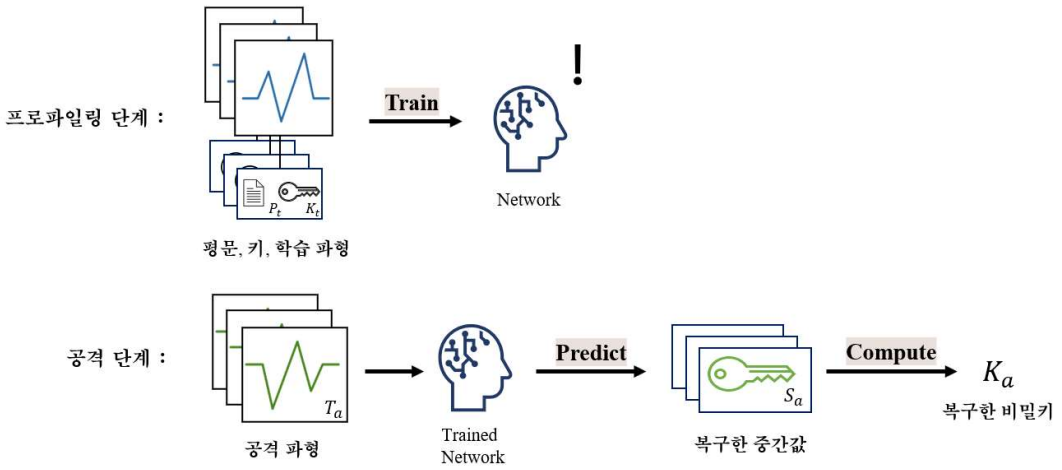
[4 - 3 문제 (70점)]

AES-128에 딥러닝 기반 프로파일링 부채널 분석을 적용하여 마스터키를 복구하라!

딥러닝 기반 프로파일링 부채널 분석은 공격자가 공격하고자 하는 장비와 유사하고 완전히 제어할 수 있는 프로파일링 장비를 소유한 환경을 가정한다. 공격은 프로파일링 장비를 통해 수집한 부채널 정보를 이용하여 신경망 학습을 수행하는 프로파일링 단계와 실제 대상 장비로부터 수집된 부채널 정보와 학습된 신경망을 사용해 비밀키를 복구하는 공격 단계로 구성된다. 각 단계에 대한 자세한 설명은 다음과 같다.

프로파일링 단계에서는 공격자가 소유한 프로파일링 장비를 이용하여 임의의 평문과 키에 대해 암호 알고리즘이 동작할 때 발생하는 부채널 정보를 수집한다. 이때 실질적으로 유의미한 시점의 정보를 추출하여 부채널 정보의 특성을 모델링한다. 즉, 수집한 부채널 정보를 입력값으로, 부채널 정보에 대응하는 중간값을 라벨로 사용하여 인공 신경망을 학습시킨다. 이때 학습에 영향을 주지 않는 선에서 신경망의 정확도를 판단하기 위하여 수집한 부채널 정보 중 일부를 검증 데이터 집합으로 사용한다.

공격 단계에서는 프로파일링 단계에서 학습된 인공 신경망을 사용하여 비밀 정보를 복구한다. 공격 장비에서 얻은 부채널 정보를 입력으로 하였을 때 얻은 신경망의 결과를 바탕으로 중간값을 복원하고 그에 대응하는 비밀키를 얻을 수 있다. 이때, 가장 많이 히팅된 후보 키를 비밀키라고 추측한다. 예를 들어, 1,000개의 공격 파형을 학습된 신경망의 입력으로 넣었을 때 각 공격 파형에 대응되는 신경망의 중간값을 얻을 수 있다. 그러한 중간값들을 일련의 과정을 거쳐 후보 키로 복원했을 때, 1,000개의 복원 값들 중 가장 많이 나타난 후보 키를 비밀키라고 판단한다.



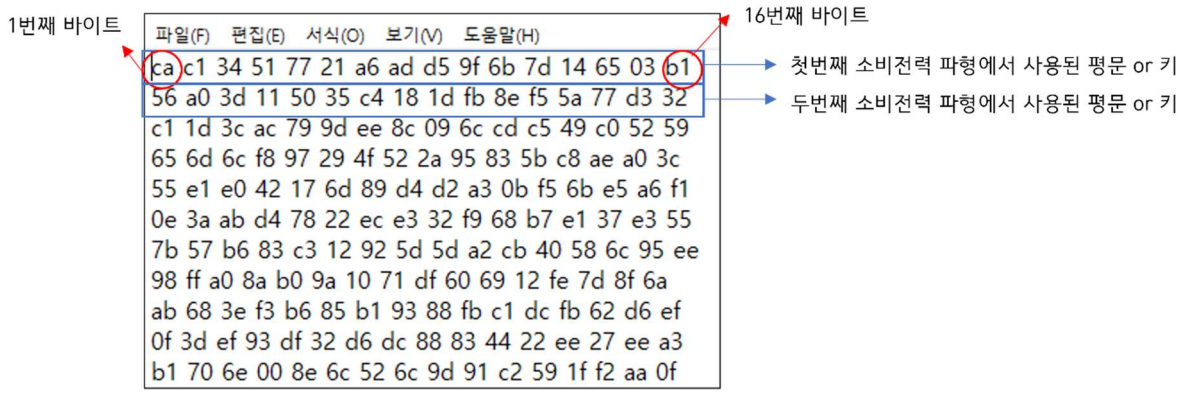
본 문제는 AES-128이 동작할 때 발생하는 소비전력 파형을 사용하여 최종적으로 AES-128에서 사용된 마스터키를 복구하는 문제이다.

딥러닝 기반 프로파일링 부채널 분석을 위해 제공되는 학습파형과 공격파형 모두 동일한 장비에서 수집하였으며, 이때 두 파형 모두 AES-128의 3Round(AddRoundKey, SubBytes, ShiftRows, MixColumns)가 동작할 때의 소비전력 파형이다.

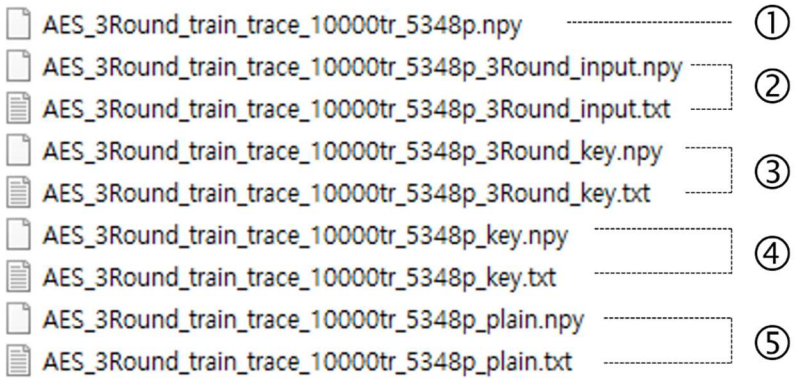
제공한 파일에 대한 설명은 다음과 같다.

1) AES_Train

AES_Train 폴더에는 프로파일링 단계에서 사용하는 소비전력 파형, 평문, 키에 대한 정보가 담겨 있다. 확장명 npy는 파이썬의 NumPy (NPY) 파일 형식으로 저장된 배열이 포함되어 있으며, numpy 모듈을 통해 사용할 수 있다. 확장명 txt는 npy에 저장된 배열을 다음의 그림과 같이 저장한 파일이다.



제공된 파일은 총 9개이며 파일에 따른 설명은 다음과 같다.



① AES-128의 3Round의 소비전력 파형이다. 총 10,000개의 파형이 담겨 있으며 각 파형 모두 5,348 point로 이루어져 있다.

② AES-128 소비전력 파형에서 사용된 3Round의 AddRoundKey 입력에 대한 정보이다.

③ AES-128 소비전력 파형에서 사용된 3라운드키에 대한 정보이다.

④ AES-128 소비전력 파형에서 사용된 키에 대한 정보이다.

⑤ AES-128 소비전력 파형에서 사용된 평문에 대한 정보이다.

✌이때 ①, ④, ⑤만을 사용하여 학습할 경우 추가점수를 부여한다✌

(이 경우 사용한 코드를 추가적으로 제출해야 한다.)

2) AES_Attack

AES_Attack 폴더에는 공격단계에서 사용하는 소비전력 파형, 평문에 대한 정보가 담겨있다. 따라서 AES_Attack 폴더에 저장되어 있는 소비전력 파형의 3라운드키 전체를 복구한 후 마스터키를 복

구해야 한다.

제공된 파일은 총 2개이며 파일에 따른 설명은 다음과 같다.

① AES-128의 3 Round의 소비전력 파형이다. 총 30개의 파형이 담겨 있으며 각 파형 모두 5,348 point로 이루어져 있다.

② AES-128 소비전력 파형에서 사용된 3 Round의 AddRoundKey 입력에 대한 정보이다.

⇨ 프로파일링 단계와 공격단계 모두 제공된 파일을 전부 사용하지 않아도 분석이 가능하다!

추가적인 힌트로 AES_Attack 소비전력 파형에서 사용되는 3라운드키의 짝수번째 바이트를 공개하며 다음과 같다.

Byte	1st															16th
3 Round Key	???	0x6c	???	0x9d	???	0xcf	???	0xb1	???	0x36	???	0xf3	???	0xe6	???	0x10

답안으로 제출할 것은 다음과 같다.

1. 3라운드키 복구를 위한 딥러닝 기반 프로파일링 부채널 분석 학습 및 공격 논리
   (아주 아주 아주 자세하게 작성!)
2. 프로파일링 단계에 사용된 신경망 구조
   (최대한 자세하게 작성, 이러한 신경망을 사용한 이유도 넣으면 아주 좋음)
3. 사용된 소스코드 및 그림
   그림은 아래와 같이 프로파일링/공격 단계에 따라 바이트별로 모두 출력하여 제출한다.
   - ✓ 프로파일링 단계 - 에폭에 따른 Loss, Accuracy 추이 그래프 그림
     (만약 검증집합을 사용했을 경우 Validation Loss, Validation Accuracy도 출력한다.)
   - ✓ 공격 단계 - 공격 파형을 사용했을 때 후보키에 따른 키 히팅 수 그림
     (중요 : 이때 가장 높은 히팅 수를 가지는 키의 히팅 수도 출력한다.)
4. 복구한 3라운드키 및 마스터키

● 참고 사항

1) AES-128 표준문서: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf
2) SPA(Simple Power Analysis): Stefan Mangard, Power Analysis Attacks – Revealing the Secrets of Smart Cards. Chapter 5.2 Visual Inspections of Power Traces
3) Martinasek, Zdenek, and Vaclav Zeman. "Innovative method of the power analysis." Radioengineering 22.2 (2013): 586-594

문의: KMU.PEPSI @gmail.com