파형 분석을 통한 암호 분류 인공지능 모델

정보컴퓨터공학과 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

ChipWhisperer 파형 수집

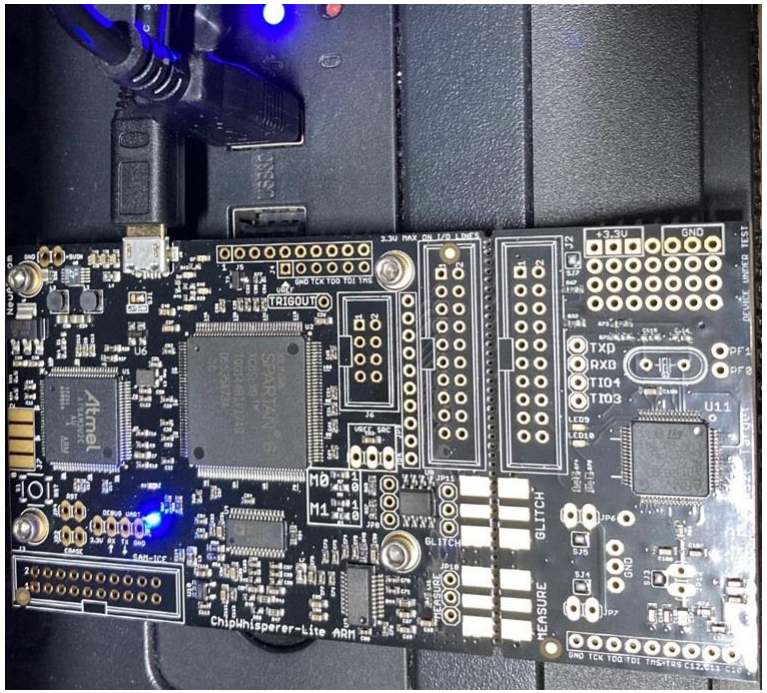
모델 구성

성능 평가

결론

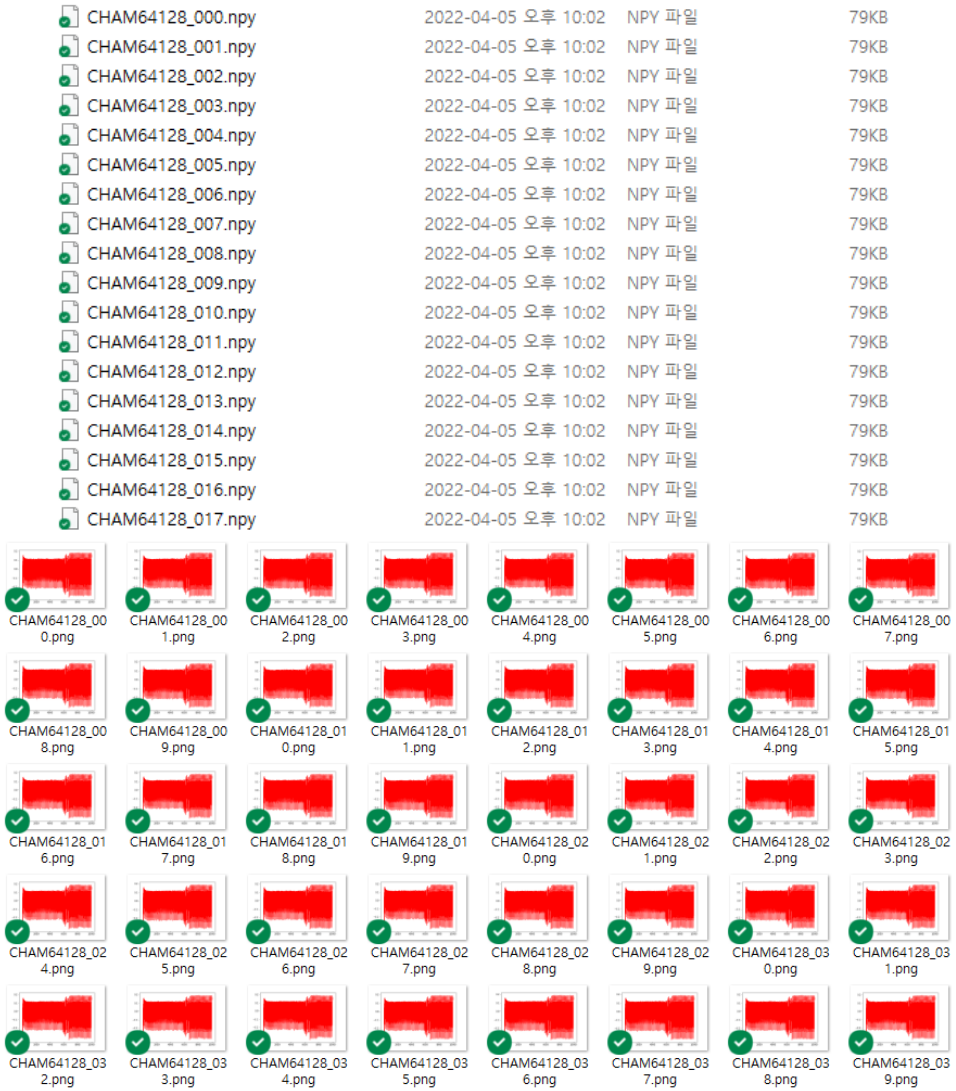
ChipWhisperer 파형 수집

- ChipWhisperer를 사용하여 파형 수집
- 파형 샘플의 수는 10,000개
- 파형의 수는 5,000개
- 대상 암호 알고리즘 (총 9종)
  - AES-128
  - CHAM-64/128, 128/128, 128/256
  - LEA-128, 192, 256
  - PIPO-64/128, 64/256
- 수집한 파형을 **JPG**와 **NPY** 데이터로 저장



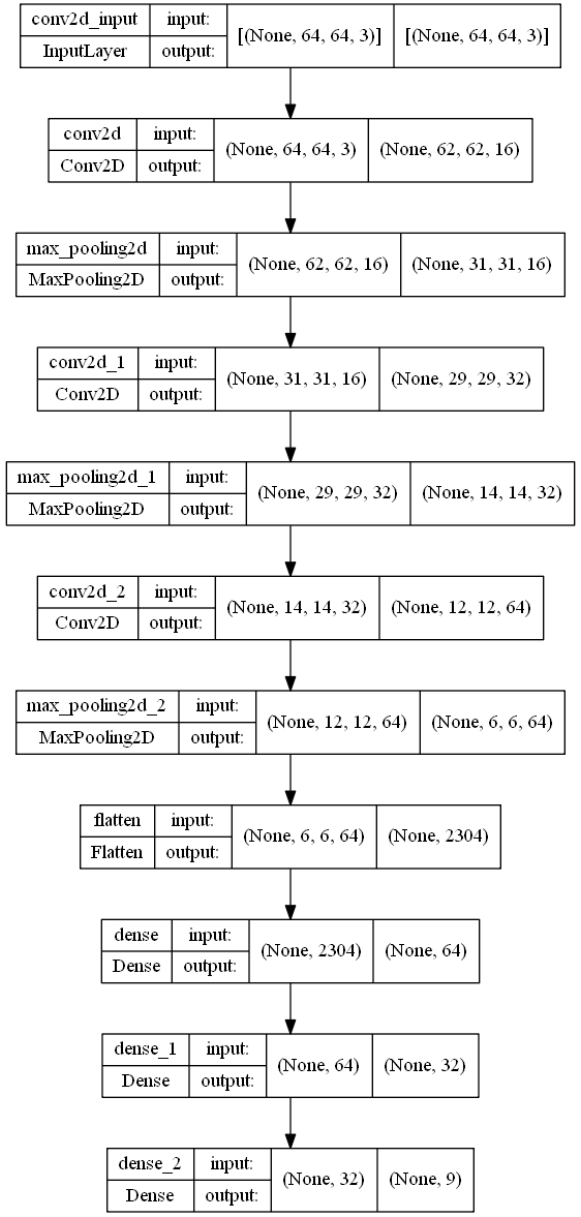
ChipWhisperer 파형 수집

- 수집된 데이터를 일정 비율로 분리
  - 6(train):2(validation):2(test)
- 총 데이터의 수
  - Train: 27,000
  - Validation: 9,000
  - Test: 9,000
- 각각의 데이터를 사용하여 학습 진행



모델 구성

- 파형 이미지를 사용하여 학습을 위해 **CNN** 구축
- Sequential 형태로 레이어를 쌓음
  - Convolution 레이어 3개
  - Dense 레이어 2개
  - Dropout 레이어 2개 (optional)
  - Activation: relu, softmax
  - Loss: categorical crossentropy
  - Optimizer: adam
- **파라미터(하이퍼 파라미터) 조절로 여러 모델 생성**
  - 뉴런 수 조절, Dropout 레이어 추가
  - 총 4종의 모델 생성



성능 평가

종류	파라미터 수	학습 정확도	학습 손실	검증 정확도	검증 손실	시험 정확도
1	173,481	93.10%	0.125	94.38%	0.108	92.19%
2	173,481 + Dropout	77.90%	0.452	85.00%	0.167	88.75%
3	1,303,305	90.60%	0.152	93.12%	0.136	93.44%
4	1,303,305 + Dropout	90.35%	0.142	92.50%	0.122	90.62%

- 1은 전체적으로 정확도가 높음
- 2는 1에 **Dropout**을 추가한 모델로, 정확도가 내려감
  - **1은 과적합**이 되었다고 판단 가능
- 3은 1에서 파라미터를 늘린 모델로 가장 좋은 시험 정확도를 보임
- 4는 3에 Dropout을 추가한 모델로, 정확도가 거의 유지됨
- 3이 가장 효과적인 모델임을 알 수 있음

결론

- 적은 파라미터를 지니면 과적합 발생
  - **Dropout 레이어를 통해서 과적합 회피** 가능
- 많은 파라미터를 지니면 과적합을 피하고 높은 정확도를 보유
  - **학습에 시간이 오래 소요되며 모델이 무거워짐**
- 더 높은 학습률(**최대 98%**)을 달성하기 위한 파라미터 조절 필요
- NPY 데이터를 사용한 학습 모델 제시
  - JPG를 사용한 모델과 비교
  - 어느 데이터를 사용한 모델이 효과적인지 판단 가능

Q & A