다중 작업 학습을 이용한 딥러닝 기반 부채널 분석 연구

2020 정보보호학회 하계학술대회
Conference on Information Security and Cryptography-Summer 2020
(CISC-S 2020)

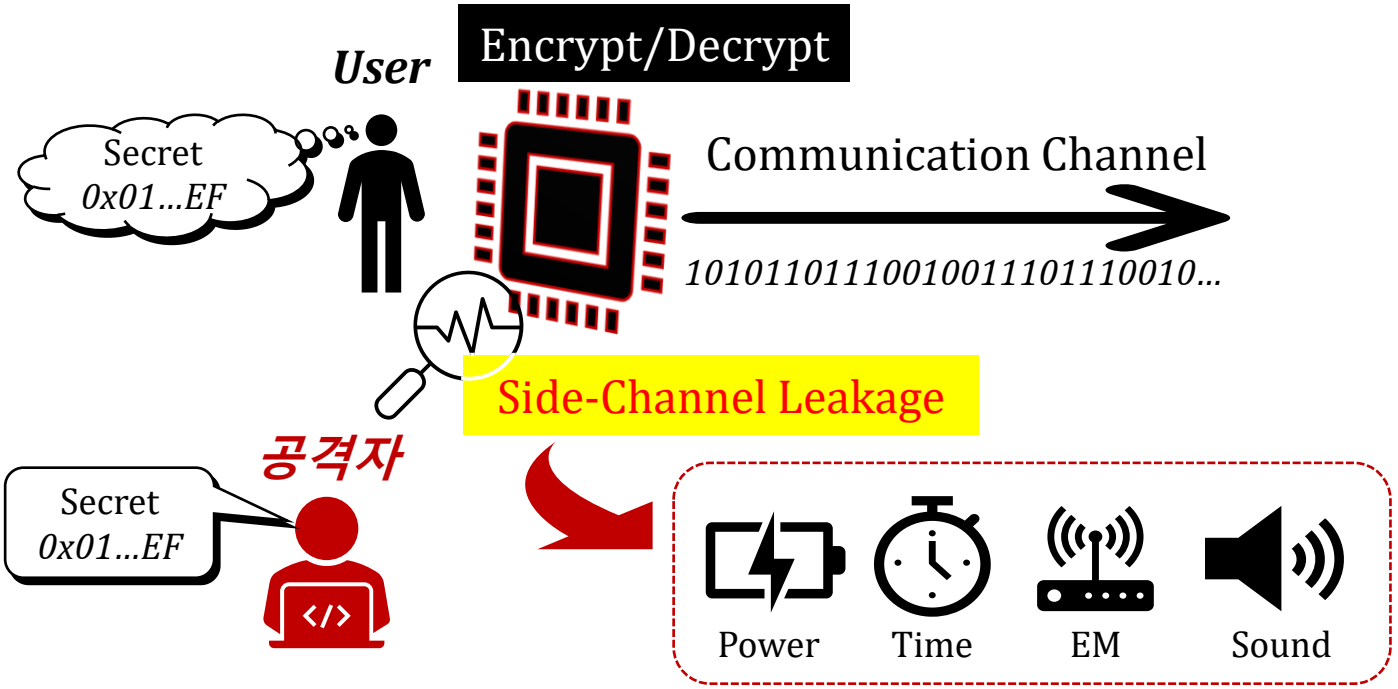
고려대학교

진성현, 김희석, 홍석희

Contents

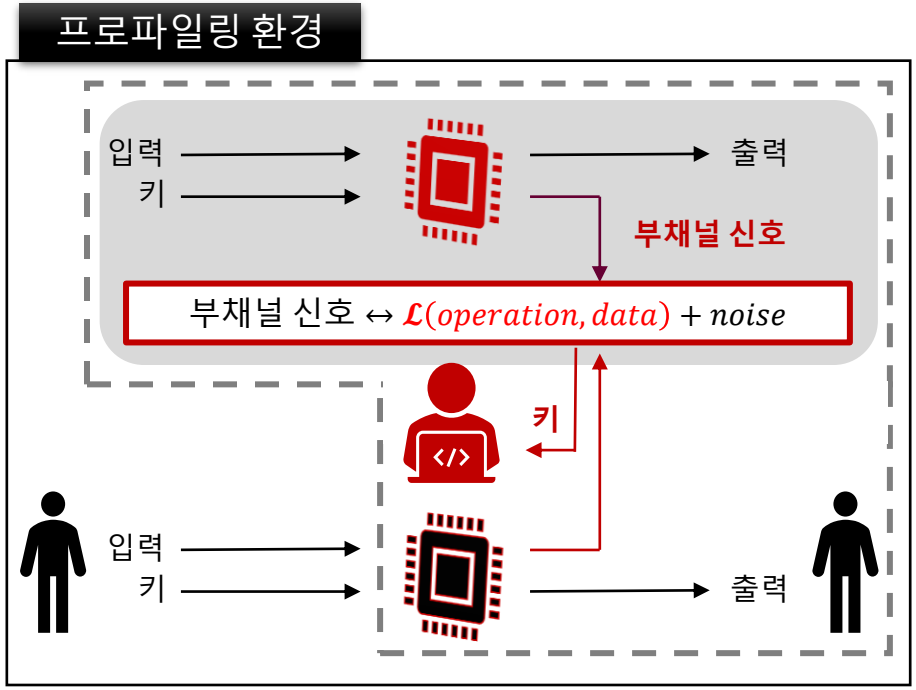
부채널 분석
Side-Channel Analysis

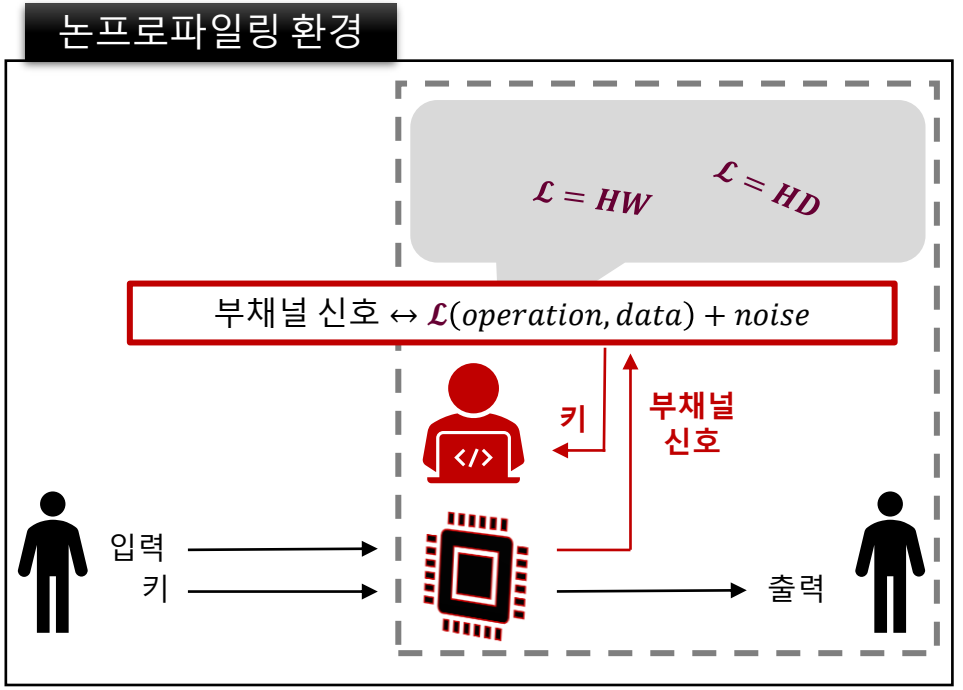
- 전자기기에서 암호를 운용할 때, 의도된 입출력인 평문/암호문 외에 설계자가 고려하지 못한 부채널 누출정보(Side-Channel Leakages) 발생



- 부채널 분석이란 부채널 신호를 이용하여 비밀정보를 분석하는 기법

부채널 분석
Side-Channel Analysis





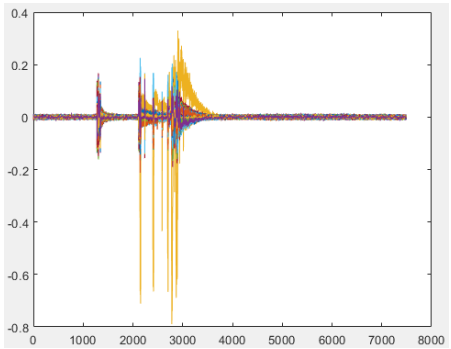
- 공격 대상 장비와 동일한 장비를 이용하여 데이터에 따른 부채널 신호 특성 분석 가능
- 강한 공격자 환경

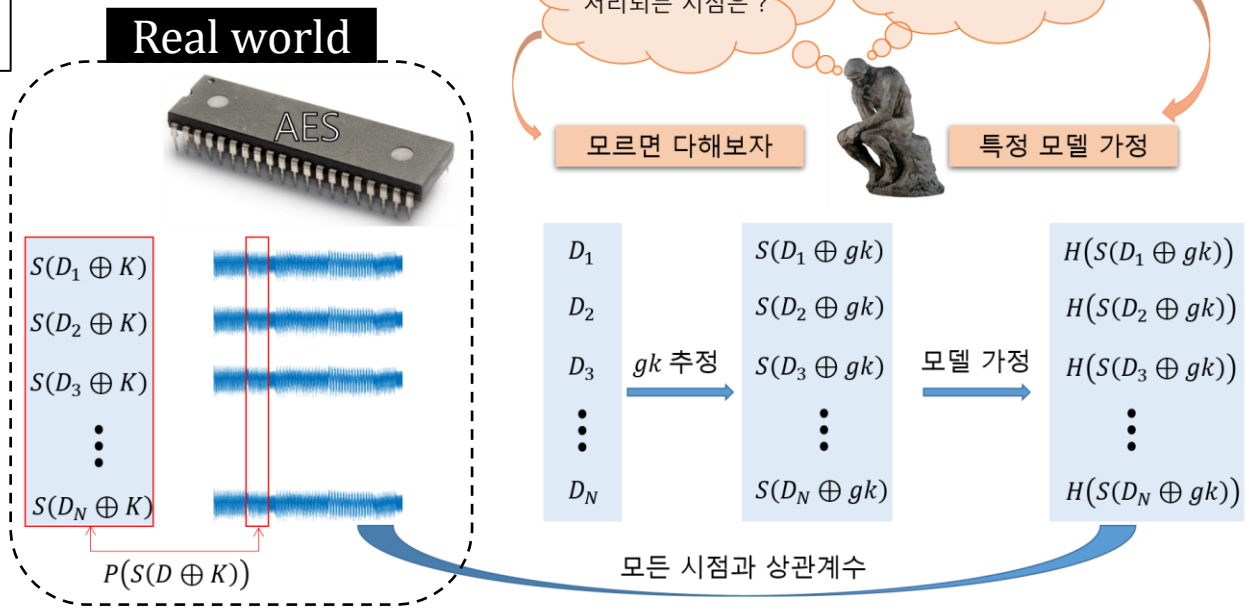
- 공격 대상 장비만을 가지고 분석
- 데이터에 따른 부채널 신호 모델 가정
- 약한 공격자 환경

상관 전력 분석
Correlation Power Analysis

- 대표적인 논프로파일링 부채널 분석 기법
  - Brier, Eric, Christophe Clavier, and Francis Olivier. "Correlation power analysis with a leakage model." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2004.

$$Corr(P,H) = \frac{COV(P,H)}{\sigma_P \cdot \sigma_H}$$





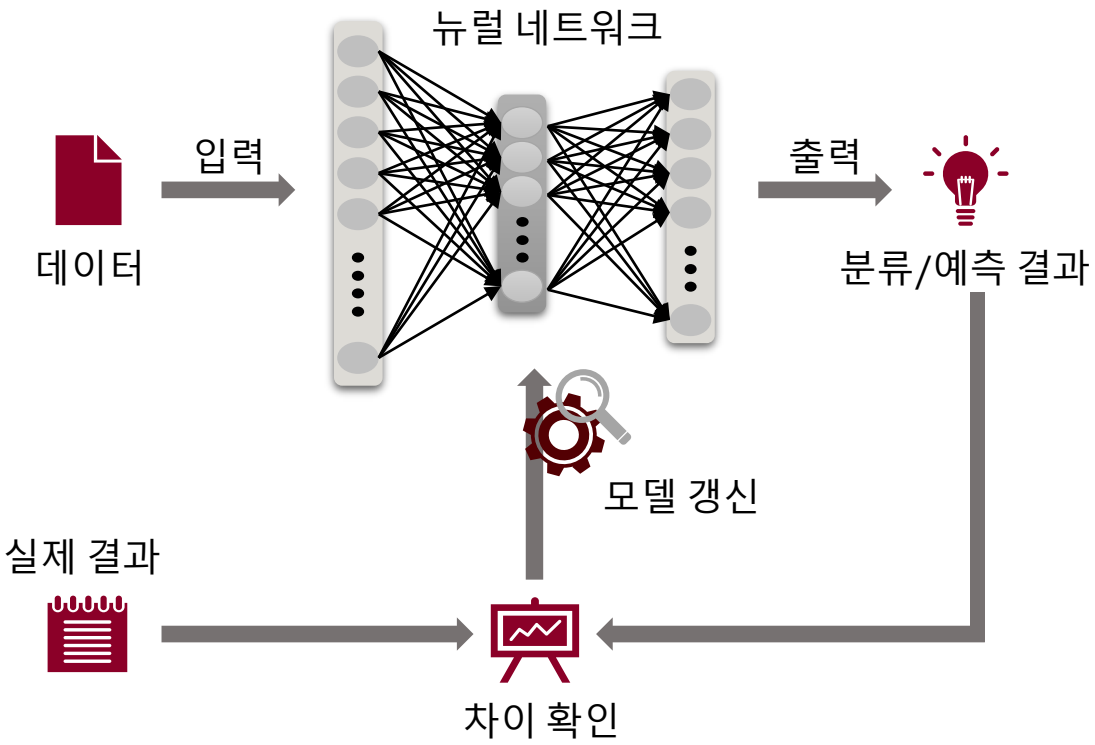
- 한계점

1. 전력 모델 가정 필요
2. 키 추측 시 한 시점의 절대적 수치만 고려됨
   ⇒ 모든 이용 가능한 정보가 활용되지 않음

Cryptographic Algorithm Laboratory

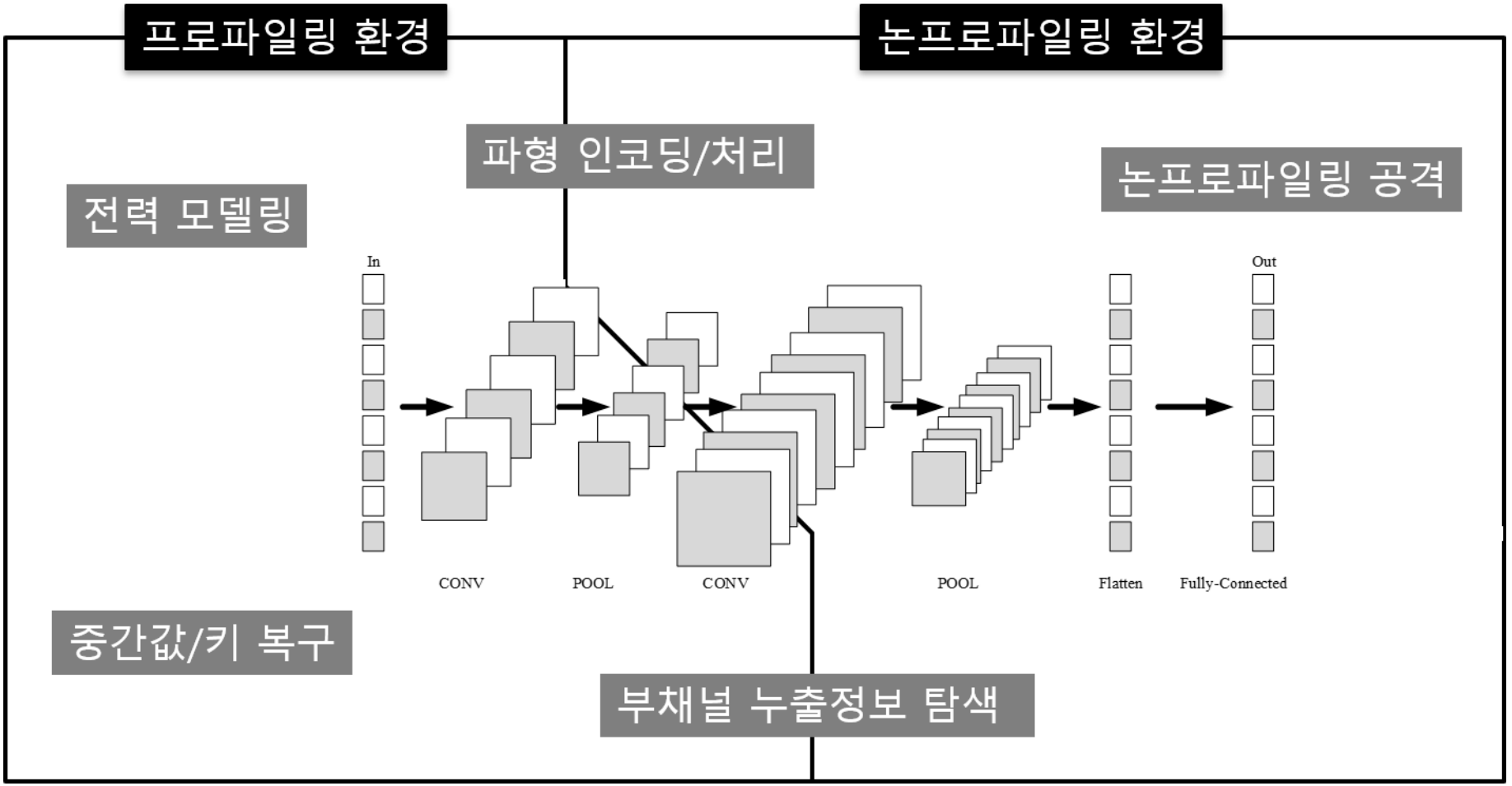
딥 러닝
Deep Learning

- 여러 개의 연산층을 통해 데이터를 순차적으로 추상화하여 의도한 작업 수행
- 특징을 자체적으로 학습이 가능하기 때문에 선별할 필요 없음
- 다량의 학습 데이터를 필요로 함



딥 러닝 기반 부채널 분석

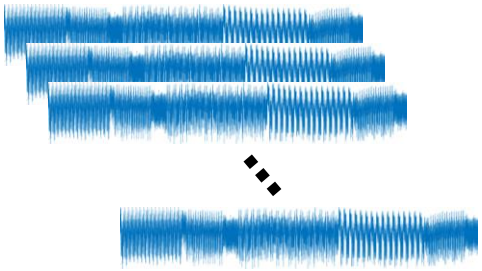
Deep Learning-based Side-Channel Analysis



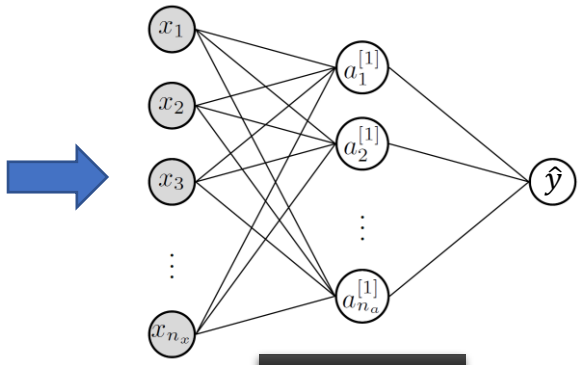
진성현, and 김희석. "딥러닝을 이용한 부채널 분석 기술 연구 동향." 정보보호학회지 30.1 (2020): 43-53.

상관성 최적화
Correlation Optimization

- 상관 분석의 성능이 높아지도록 파형을 인코딩하는데 신경망을 사용
  - Robyns, P., Quax, P., & Lamotte, W. (2018). Improving CEMA using Correlation Optimization. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(1), 1-24.



원본 파형



인코딩된 파형

손실함수

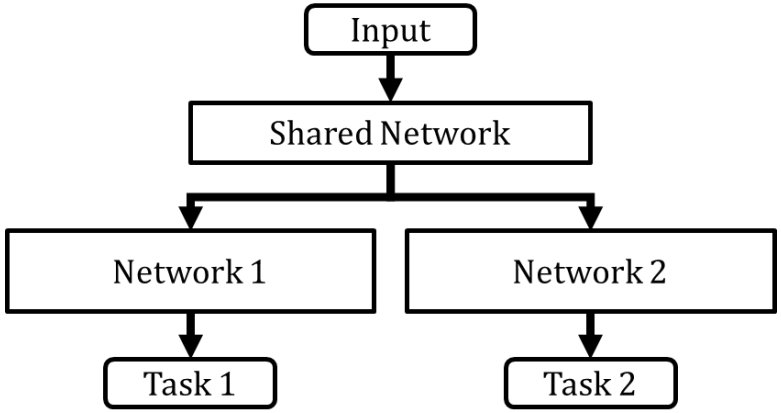
$$\mathcal{L}(\hat{y}_k, y_k) = 1 - \frac{cov(\hat{y}_k, y_k)}{\sigma_{\hat{y}_k}\sigma_{y_k} + \epsilon}$$

Negative correlation: loss → 2
No correlation: loss is 1
Positive correlation: loss → 0

특징
1. 파형의 모든 시점 정보를 이용하도록 학습
2. 전력모델 가정없이도 학습 가능
3. 주파수 도메인 이용시 (shallow) MLP로 미정렬 파형 분석 가능

다중 작업 학습
Multi-Task Learning

- 하나의 신경망이 여러 작업을 동시에 수행하도록 하는 방법



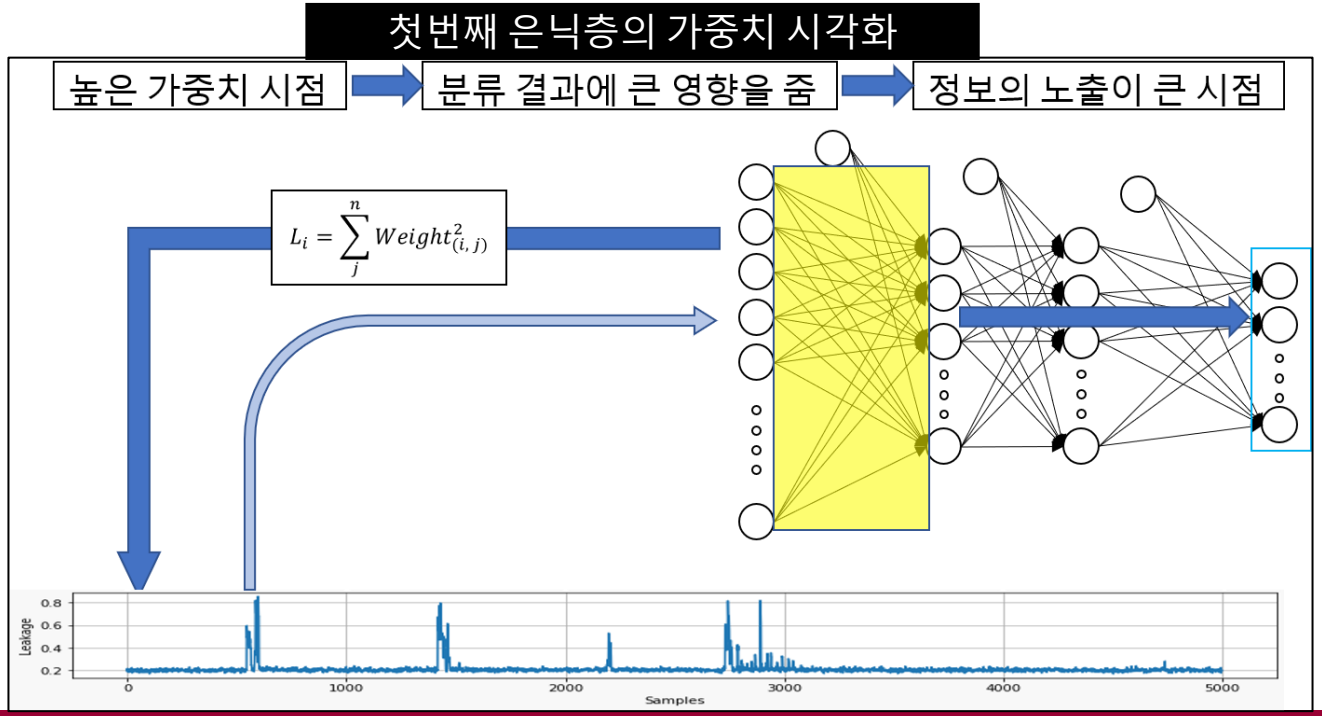
- 다중 작업 학습을 하는 경우
  - 여러 문제들에 대해 데이터들이 저레벨 특성을 공유할 때

    ex) 컴퓨터 비전에서 객체 분류
  - 다중 작업들을 하나의 큰 신경망으로 한번에 학습 시키려고 할 때
- 다중 작업 학습이 가능하도록 신경망이 충분히 커야함

다중 작업 학습을 이용한 딥러닝 기반 부채널 분석

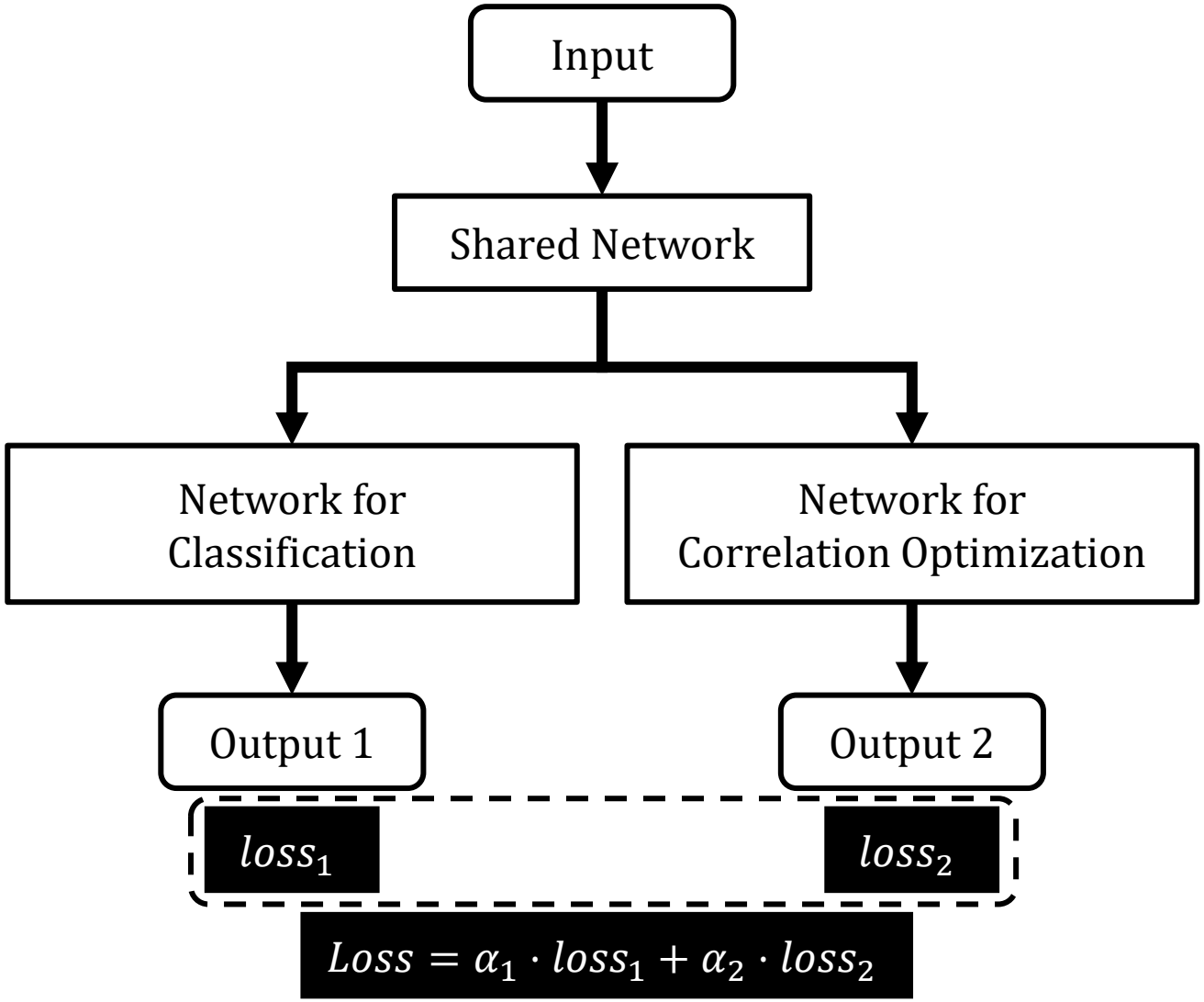
Deep Learning-based Side-Channel Analysis with Multi-Task Learning

- Idea : 여러 딥러닝 기반 부채널 분석을 하나의 신경망으로 다중 작업
  - 신경망은 동일한 파형으로부터 특정 작업을 위한 출력을 하도록 학습됨
    - 중간값 분류, 딥러닝 차분 분석, 상관성 최적화, ...
  - 각 기법은 특정 부분키를 분석하기 위해 관련 누출 시점들을 이용
    - 사용하는 시점이 동일하거나 유사할 것으로 기대 가능



다중 작업 학습을 이용한 딥러닝 기반 부채널 분석

Deep Learning-based Side-Channel Analysis with Multi-Task Learning



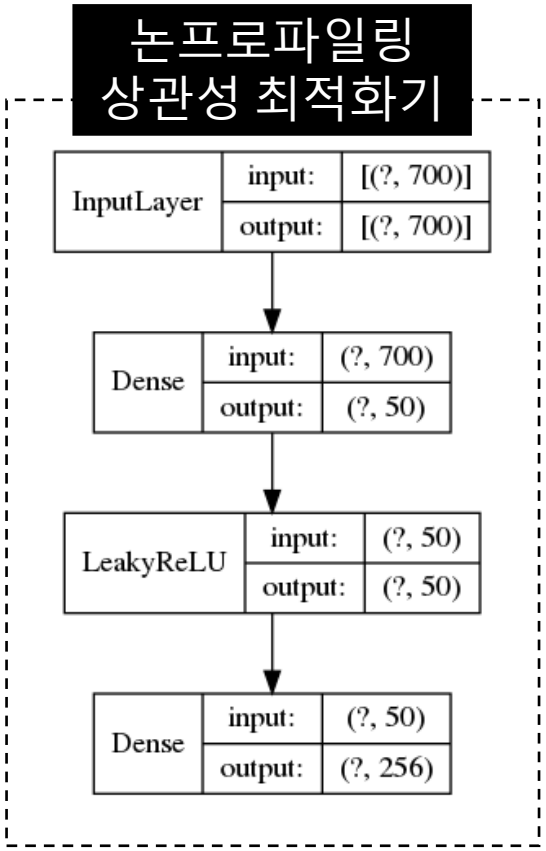
실험 결과
Experimental Results

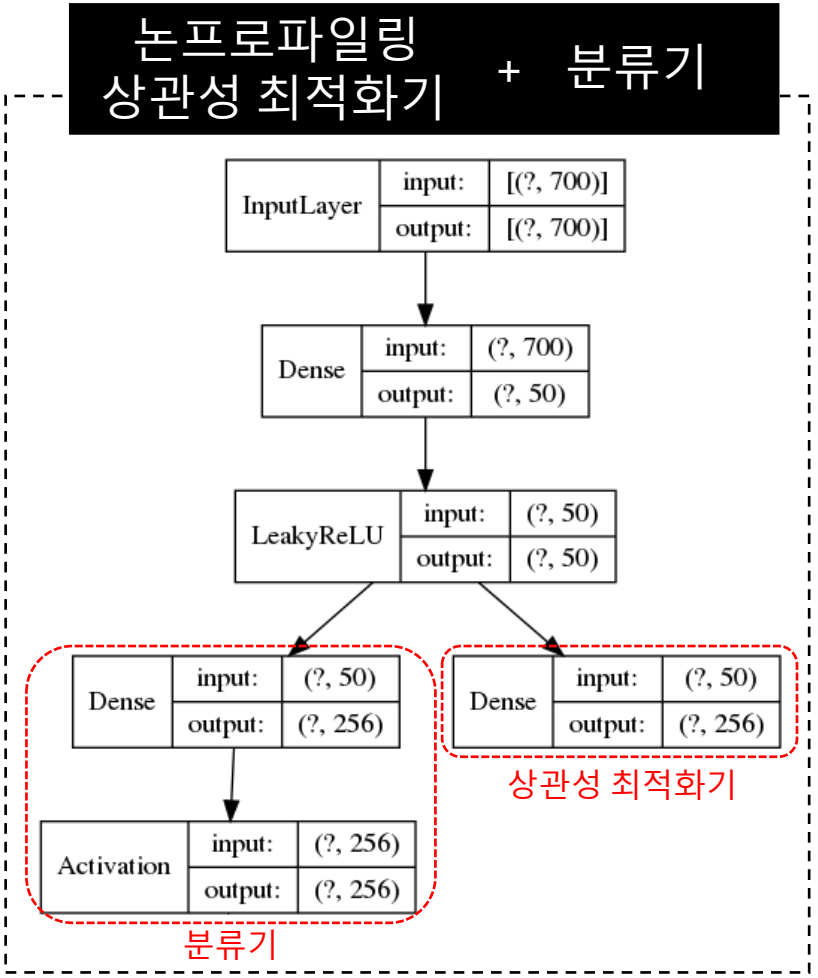
- Case : 논프로파일링 상관성 최적화기 성능 향상을 위한 (중간값) 분류기 이용

- ASCAD_sync
  - 8-bit ATmega8515 칩에서 1차 마스킹된 AES 고정키 암호화에 대한 데이터셋
  - 학습/테스트 데이터셋 : 50,000/10,000
  - 다중 작업 학습의 성질만 분석하기 위해 정렬된 데이터셋 이용

- 구현
  - Tensorflow v2.1의 고수준 API인 Keras 이용

실험 결과
Experimental Results



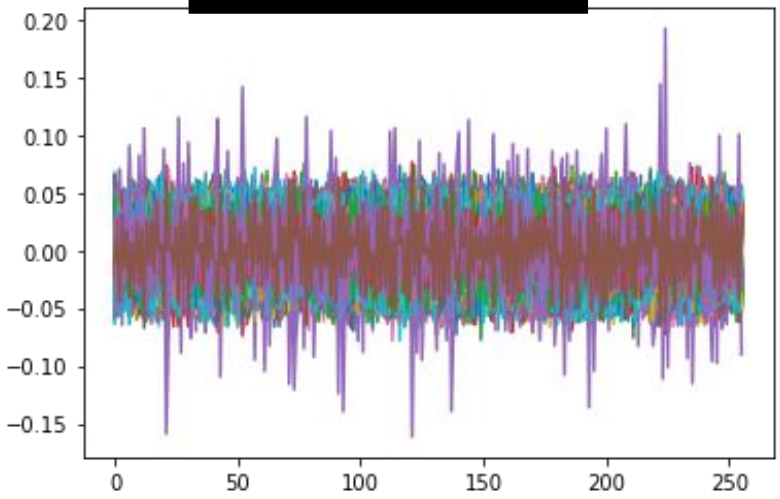


Note
논프로파일링 상관성 최적화기도
다중 작업 학습의 일종으로 간주 가능

실험 결과
Experimental Results

- CPA 결과

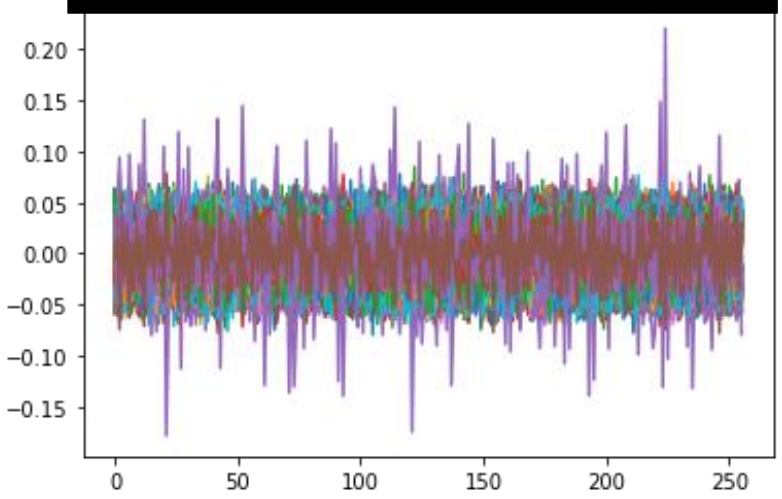
논프로파일링
상관성 최적화기



0xE0
0.19214
2.37091

1st guess key
max peak
confidence

논프로파일링
상관성 최적화기 + 분류기



0xE0
0.22036
2.59191

Cryptographic Algorithm Laboratory

결론

- 딥러닝 기반 부채널 분석에서 다중 작업 학습 제안
- 특정 작업의 성능 향상 가능함을 확인

- Future works
  - 다른 딥러닝 기반 부채널 분석들에 대한 다중 작업 학습 적용 연구
  - 전이 학습(Transfer Learning)을 이용한 딥러닝 기반 부채널 분석 연구


LIBERTAS JUSTITIA VERITAS
KOREA UNIVERSITY
1905
ALHM
Cryptographic
Algorithm Laboratory
Q&A
Thanks