Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.1271

지터에 강건한 딥러닝 기반 프로파일링 부채널 분석 방안*

김 주 환,[1†] 우 지 은,[2] 박 소 연,[2] 김 수 진,[2] 한 동 국[3‡]
[1]국민대학교 수학과 (학생), [2]국민대학교 정보보안암호수학과 (학생),
[3]국민대학교 금융정보보안학과 (교수)

Robust Deep Learning-Based Profiling Side-Channel Analysis for Jitter*

Ju-Hwan Kim,[1†] Ji-Eun Woo,[2] So-Yeon Park,[2] Soo-Jin Kim,[2] Dong-Guk Han[3‡]
[1]Department of Mathematics, Kookmin University (Undergraduate),
[2]Department of Information Security, Cryptology, and Mathematics,
Kookmin University (Undergraduate),
[3]Department of Financial Information Security, Kookmin University (Professor)

요 약

딥러닝 기반 프로파일링 부채널 분석은 신경망을 이용해 부채널 정보와 중간값의 관계를 파악하는 공격 방법이다. 신경망은 신호의 각 시점을 별도의 차원으로 해석하므로 차원별 가중치를 갖는 신경망은 지터가 있는 데이터의 분포를 학습하기 어렵다. 본 논문에서는 CNN(Convolutional Neural Network)의 완전연결 층을 GAP(Global Average Pooling)로 대체하면 태생적으로 지터에 강건한 신경망을 구성할 수 있음을 보인다. 이를 입증하기 위해 ChipWhisperer-Lite 전력 수집 보드에서 수집한 파형에 대해 실험한 결과 검증 데이터 집합에 대한 완전연결 층을 사용하는 CNN의 정확도는 최대 1.4%에 불과했으나, GAP를 사용하는 CNN의 정확도는 최대 41.7%로 매우 높게 나타났다.

ABSTRACT

Deep learning-based profiling side-channel analysis is a powerful analysis method that utilizes the neural network to profile the relationship between the side-channel information and the intermediate value. Since the neural network interprets each point of the signal in a different dimension, jitter makes it much hard that the neural network with dimension-wise weights learns the relationship. This paper shows that replacing the fully-connected layer of the traditional CNN (Convolutional Neural Network) with global average pooling (GAP) allows us to design the inherently robust neural network inherently for jitter. We experimented with the ChipWhisperer-Lite board to demonstrate the proposed method: as a result, the validation accuracy of the CNN with a fully-connected layer was only up to 1.4%; contrastively, the validation accuracy of the CNN with GAP was very high at up to 41.7%.

Keywords: Side-Channel Analysis, Deep Learning, Jitter, Global Average Pooling, AES

I. 서 론

프로파일링 부채널 분석(profiling side-channel analysis)은 부채널 정보와 중간값의 관계를 사전에 프로파일링하여 적은 정보로도 비밀키를 복구할 수 있는 강력한 분석 방법이다. 전통적인 프로파일링 부채널 분석은 통계적 모델을 사용해 부채널 정보와 중간값의 관계를 파악한다[1, 2]. 전통적인 방식은

Received(10. 12. 2020), Modified(12. 03. 2020)
Accepted(12. 03. 2020)
* 본 논문은 산업통상자원부 국제공동기술개발사업으로 지원된 연구임.(P0011922, 딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발)
† 주저자, zzzz2605@kookmin.ac.kr
‡ 교신저자, christa@kookmin.ac.kr(Corresponding author)

데이터에 적합한 모델을 분석자가 선택해야 하며, 전체 신호 중 중간값과 관련된 관심 영역(Point of Interst, PoI)을 선택해야 하는 등의 전처리가 필요하다. 따라서 이 방식은 분석자의 능력에 따라 결과가 크게 좌우되며, 일반적으로 높은 성능을 기대하기 어렵다. 최근 이러한 문제를 완화하기 위해 신경망을 이용하는 분석 방법이 제안되었다[3, 4, 5]. 범용 근사자(universal approximator)[6]인 신경망은 학습을 통해 데이터에 적합한 관계식을 스스로 찾을 수 있고, 입력 중 중간값과 관련된 영역을 찾아낸다. 따라서 신경망을 이용하는 분석 방법은 분석자의 능력에 비교적 적게 의존하며, 전통적인 방식에 비해 높은 성능을 갖는다.

신호가 시간축상으로 흔들리는 현상인 지터는 부채널 분석을 방해하는 주요 요소이다. 특히 신경망은 신호의 각 시점을 별도의 차원으로 해석하므로, 지터가 있으면 특징(feature)의 차원이 빈번히 반전되는 효과가 발생한다. 따라서 특징 벡터(feature vector)의 차원별로 독립적인 가중치를 갖는 신경망인 MLP(Multi-Layer Perceptron)[7]는 지터가 있는 데이터의 관계를 파악하기 어렵다. 반면, CNN(Convolutional Neural Network)[8]은 구조적 특성 덕분에 지터가 있는 데이터를 효과적으로 분석할 수 있음이 알려졌다[9, 10]. 그러나, LeNet-5[8] 기반의 전통적인 CNN 구조는 종단에 분류를 위해 MLP와 동일한 구조인 완전연결 층(fully-conncted layer)을 사용하므로 여전히 지터의 영향을 받는다. 본 논문에서는 CNN이 지터에 민감하게 만드는 주요 원인인 완전연결 층을 GAP(Global Average Pooling)[11]로 대체하면 지터에 강건한 신경망을 구성할 수 있음을 보인다.

논문의 구성은 다음과 같다. 2장에서는 기존 연구인 지터에 내성을 갖는 프로파일링 부채널 분석 방법과 기반 지식을 다룬다. 3장에서는 GAP를 이용하여 지터에 강건한 프로파일링 부채널 분석 방법론을 제안한다. 4장에서는 ChipWhisperer-Lite 전력 수집 보드를 이용해 제안한 방법을 검증한다. 마지막으로 5장에서는 결론을 제시하며 마친다.

II. 딥러닝 기반 프로파일링 부채널 분석

2.1 Convolutional Neural Network

CNN은 LeNet-5[8]를 기반으로 발전된 신경망으로 이동이 빈번한 데이터에 적합한 구조이다. 이 신경망은 Fig. 1.과 같이 크게 컨볼루션 층(convolutional layer), 풀링 층(pooling layer), 완전연결 층으로 나눌 수 있다. 컨볼루션 층은 여러 개의 작은 커널을 이동하며 컨볼루션 연산을 수행해 특징을 추출한다. 각 커널은 위치와 무관하게 동일한 가중치를 사용하므로 데이터의 이동 정보가 특징 맵(feature map)에 그대로 반영되는 특성이 있다. 즉, 컨볼루션 층은 이동에 동변(translation equivariant)인 특성이 있다. 풀링 층은 인접한 원소들의 통계적 대푯값을 추출하여 정보를 압축한다. 대푯값을 추출하면 특징의 불변성을 찾을 수 있으므로 데이터의 이동을 극복할 수 있다. 풀링에는 통계량으로 최댓값을 사용하는 최대 풀링(max pooling)과 평균값을 사용하는 평균 풀링(average pooling)이 있다. 마지막으로 완전연결 층은 MLP와 동일한 구조로, 입력의 차원별로 다른 가중치를 갖는다. 따라서 데이터의 이동에 민감한 특성이 있다.

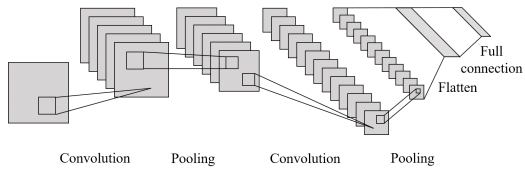


Fig. 1. Traditional CNN architecture

2.2 딥러닝 기반 프로파일링 부채널 분석

프로파일링 부채널 분석은 부채널 정보와 중간값의 관계를 프로파일링하여 소수의 파형으로도 비밀키를 복구할 수 있는 강력한 분석 방법이다. 분석자는 목표 장비와 동일하며 완전히 통제할 수 있는 프로파일링 장비를 이용해 얻은 다량의 파형으로 프로필을 생성한 뒤, 목표 장비에서 수집한 소수의 파형으로 비밀키를 복구한다. 구체적으로 프로파일링 분석은 다음과 같이 프로파일링 단계와 비밀키 복구 단계로 나누어 수행한다.

1. [프로파일링 단계]
   프로파일링 장비에서 임의의 평문을 암호화할 때 얻은 다량의 파형과 중간값을 이용해 파형과 중간값의 관계를 모델링 한다. 즉, 프로필을 생성한다.
2. [비밀키 복구 단계]
   미리 생성한 프로필을 이용해 목표 장비에서 얻은

소량의 파형에 대응되는 중간값을 예측한다. 예측한 중간값과 평문을 조합하여 비밀키를 복구한다.

딥러닝 기반 프로파일링 부채널 분석에서는 파형과 중간값의 관계를 모델링 하기 위해 신경망을 활용한다. 즉, 다음과 같이 프로파일링 분석을 수행한다.

1. 〔학습 단계〕
   프로파일링 장비에서 임의의 평문을 암호화할 때 얻은 다량의 파형을 특징, 중간값을 목푯값(label)으로 하여 신경망을 학습시킨다.
2. 〔비밀키 복구 단계〕
   학습된 신경망을 이용해 목표 장비에서 얻은 소량의 파형에 대응되는 중간값을 예측한다. 예측한 중간값과 평문을 조합하여 비밀키를 복구한다.

프로파일링 분석의 성능을 측정하는 대표적인 지표는 추측 엔트로피(guessing entropy)와 성공률(success rate)이다〔12〕. 추측 엔트로피는 분석 결과로 얻은 확률을 내림차순으로 정렬했을 때, 옳은 키 순위의 평균으로 정의하며, 성공률은 옳은 키 순위가 1위일 경험적 확률로 정의한다.

2.3 지터에 내성을 갖는 프로파일링 부채널 분석

딥러닝에서 지터는 특징의 차원이 반전되는 효과로 해석된다. 차원별로 다른 가중치를 갖는 신경망에게 지터는 데이터의 분포가 수시로 바뀌는 효과를 낸다. 즉, 그래디언트(gradient)의 방향이 일정하지 않도록 만듦으로써 학습에 악영향을 준다. 기존 연구〔10〕는 인접한 정보를 압축하여 신경망이 데이터의 작은 이동을 감내할 수 있게 하는 풀링 층의 특성을 활용하여 신경망이 지터에 내성을 갖도록 설계하는 방안을 제안하였다.

풀링 층의 커널의 크기가 p이고 보폭이 커널의 크기와 같으면 풀링 층을 한 번 거칠 때마다 p차원의 특징 벡터가 1차원으로 축소된다. 따라서 l개의 풀링 층을 거치면 특징의 p^l차원이 1차원으로 요약된다. 파형이 최대 z포인트 이동할 때, 수식 (1)을 만족하도록 신경망을 구성하면 입력의 z포인트가 완전연결 층 입력의 1차원으로 집약되므로 신경망이 지터에 내성을 갖는다.

$$p^l > z \Leftrightarrow l > \log_p z \tag{1}$$

기존 연구는 데이터의 이동 폭이 넓어지면, 즉 z가 증가하면 신경망을 깊게 구성하거나, 커널의 크기를 증가시켜야 한다. 신경망이 깊어지면 용량이 증가해 과적합(overfitting)이 발생할 수 있고, 커널의 크기가 증가하면 손실되는 정보량이 증가하므로 기존 방법은 z가 작거나 데이터가 충분히 많은 경우에만 적용할 수 있는 단점이 있다.

III. 지터에 강건한 프로파일링 부채널 분석

본 장에서는 완전연결 층과 GAP의 특성을 비교하여 GAP를 사용하면 지터에 강건한 신경망을 설계할 수 있음을 보인다. 기존 연구〔10〕는 데이터의 특성에 의해 신경망의 구조가 제한되는 것과 달리, 제안한 방법은 신경망을 자유롭게 설계할 수 있다. 따라서 데이터의 특성에 적합한 구조를 채택함으로써 일반화 성능이 높은 신경망을 설계할 수 있다.

3.1 Global Average Pooling

전통적인 CNN은 분류를 위해 종단에 완전연결 층을 사용한다. 완전연결 층은 데이터의 이동에 민감한 특성이 있을 뿐만 아니라, 많은 가중치를 가지므로 과적합을 유발하는 주요 요소가 된다. Lin 등은 이러한 완전연결 층의 문제점을 개선하기 위해 GAP를 제안했다〔11〕. GAP는 특징 맵별 평균을 출력하는 계층으로, 별도의 가중치를 갖지 않으며 부분 정보를 합치므로 입력의 이동에 강건한 특성을 갖는다. 따라서 완전연결 층을 GAP로 대체하면 데이터의 이동과 과적합에 강건한 신경망을 설계할 수 있다. Fig. 2.는 GAP를 이용하는 CNN 구조를 도식화한 것이다.

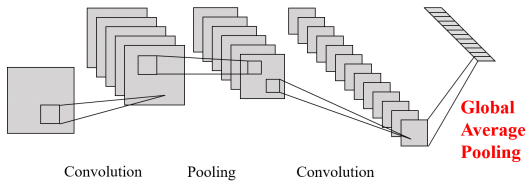


Fig. 2. The global average pooling layer

3.2 GAP의 지터에 대한 강건성 분석

본 절에서는 특징 벡터가 이동했을 때 GAP와 완전연결 층의 연산 결과를 비교하여 GAP가 지터에

강건한 특성을 가짐을 보인다.

GAP는 별도의 가중치를 갖지 않고, 단지 각 특징 맵의 통계량을 추출하므로 입력이 일부 이동하더라도 출력은 크게 변하지 않는다. 예를 들어 n차원 특징 맵 A를 오른쪽으로 p포인트만큼 이동시킨 것을 B라 하자. 즉, $n-p$이하의 임의의 자연수 i에 대해 $A_i = B_{i+p}$이다. A, B 각각을 GAP의 입력으로 넣었을 때 출력의 차는 수식 (2)와 같다. 식에서 A_i는 A의 i차원 원소를 의미한다.

$$\begin{aligned} &\mathrm{GAP}(A)-\mathrm{GAP}(B) \\ &= \frac{1}{n}\sum_{i=1}^{n}A_i - \frac{1}{n}\sum_{i=1}^{n}B_i \\ &= \frac{1}{n}\left(\sum_{i=1}^{p}A_i + \sum_{i=p+1}^{n}\boldsymbol{A_i}\right) - \frac{1}{n}\left(\sum_{i=1}^{n-p}\boldsymbol{B_i} + \sum_{i=n-p+1}^{n}B_i\right) \\ &= \frac{1}{n}\left(\sum_{i=1}^{p}A_i + \sum_{i=p+1}^{n}\boldsymbol{A_i}\right) - \frac{1}{n}\left(\sum_{i=p+1}^{n}\boldsymbol{A_i} + \sum_{i=n-p+1}^{n}B_i\right) \\ &= \frac{1}{n}\sum_{i=1}^{p}(A_i - B_{i+n-p}) \end{aligned} \quad (2)$$

위의 수식은 GAP가 원소의 위치와 무관하게 동일한 연산을 하므로 데이터가 이동하더라도 출력은 크게 변하지 않음을 의미한다. 반면, 완전연결 층에 A, B 각각을 입력했을 때 출력의 차는 수식 (3)과 같다. 식에서 $u_{i,j}$는 입력의 i차원 원소와 출력의 j차원 원소를 연결하는 가중치를 의미하며, FC는 완전연결 층을 의미한다.

$$(\mathrm{FC}(A)-\mathrm{FC}(B))_j = \sum_{i=1}^{n}u_{i,j}A_i - \sum_{i=1}^{n}u_{i,j}B_i \quad (3)$$

완전연결 층은 데이터의 위치에 따라 곱해지는 가중치가 달라진다. 즉, A_i와 B_{i+p}는 동일한 값이나, 각각에 대응되는 가중치는 각각 $u_{i,j}$, $u_{i+p,j}$로 다르다. 이 경우 데이터가 이동하면 출력이 크게 변할 수 있다. 따라서 이동에 민감한 완전연결 층 대신 GAP를 이용하면 신경망이 지터에 강건하게 구성할 수 있다.

IV. 실험 결과

본 장에서는 제안한 방법과 기존 연구[10]에 대한 비교 실험을 수행하여 제안한 방법을 적용하면 과적합에 취약하지 않으면서 지터에 강건한 신경망을 구성할 수 있음을 보인다.

4.1 실험 환경

학습 및 프로파일링 분석을 위하여 ChipWhisperer-Lite 전력수집 보드에서 소프트웨어로 구현된 AES-128[13] 암호알고리즘이 동작할 때의 소비전력을 수집했다. 학습을 위해 임의의 키로 10000번 암호화할 때의 파형을 수집했고, 이 중 9000개를 학습 데이터 집합으로, 1000개를 검증 데이터 집합으로 활용했다. 공격 데이터 집합은 학습 데이터 집합과 동일한 장비에서 고정된 키로 5000번 암호화할 때의 파형을 사용했다. 자세한 실험 환경은 Table 1.과 같다.

수집한 데이터는 지터가 거의 없으므로 파형별로 균등 분포 $u[-250, 250]$에서 선택한 임의의 정수만큼 데이터를 오른쪽으로 이동시켰다. Fig. 3.은 원본 파형과 지터를 추가한 파형을 도식화한 것으로, 학습 및 분석에는 아래의 지터가 추가된 파형을 사용했다.

Table 1. Experimental environment

Parameter	Value
Algorithm	AES-128
Target function	SubBytes
Number of traces	10000 (random key) 5000 (fixed key)
Number of points	2460
Sample rate	29.538MS/s
Validation ratio	10%

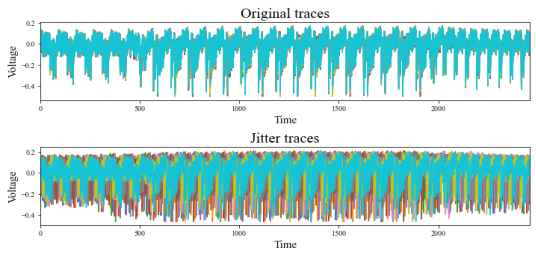


Fig. 3. Original traces and traces with an artificial jitter

4.2 신경망 설계

실험을 위해 Fig. 4.와 같이 전통적인 CNN과 GAP를 사용하는 제안한 CNN, 두 가지를 구조의 신경망을 설계했다. 완전연결 층을 GAP로 대체하면 지터에 강건한 신경망을 구성할 수 있음을 보이기 위

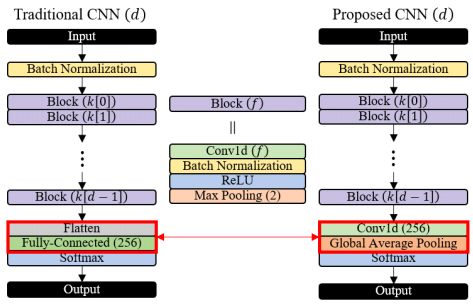


Fig. 4. Architectures of the Traditional CNN and the Proposed CNN

해 종단의 구조만 각각 완전연결 층, GAP로 다르도록 설계했다. 은닉층은 컨볼루션, 배치 정규화, 활성함수(ReLU), 풀링으로 이루어진 블록을 여러 층으로 구성하였다.

다양한 하이퍼 파라미터에서의 실험 결과를 비교하기 위해 컨볼루션 층의 커널 수 k와 깊이 d를 달리하여 실험을 수행했다. 실험에 사용한 두 종류의 커널 수 배열 k가 Table 2.와 같으며, d는 6이상 10이하의 값을 사용했다.

학습을 위해 손실 함수(loss function)는 분류 문제에서 주로 사용하는 categorical cross entropy를, 최적화 알고리즘(optimizer)으로는 Adam[14]을 사용했고, 학습률(learning rate)은 0.001, betas는 (0.9, 0.999)로 하여 200 에포크(epoch)만큼 학습을 수행했다.

Table 2. Number of kernels in each layer

Method	k
v1	[2, 4, 8, 16, 32, 64, 128, 256, 512, 1024]
v2	[8, 8, 16, 16, 32, 32, 32, 64, 64, 64]

4.3 분석 결과

$d=6$일 때 목푯값을 SubBytes 출력의 첫 번째 바이트로 하여 학습시킨 결과가 Fig. 5., Fig. 6.과 같다. Fig. 5.는 에포크별 손실(loss)을, Fig. 6.은 에포크별 정확도(accuracy)를 도식화한 것이다.

전통적인 CNN은 학습을 계속할수록 학습 데이터 집합에 대한 손실은 감소하지만, 검증 데이터 집합에 대한 손실은 증가한다. 정확도 역시 학습 데이터 집합의 정확도는 가파르게 증가하여 1에 수렴하지만, 검증 데이터 집합의 정확도는 0에서 크게 벗어나지 못한다. 즉, 일반화 성능이 떨어지는 양상을 보인다. 반면, 제안한 CNN은 학습 데이터 집합과 검증 데이터 집합 모두에 대해 손실은 감소하고 정확도는 증가하는 형태를 볼 수 있다. 이는 제안한 신경망이 지터에 강건하여 데이터의 이동에도 불구하고 파형과 중간값의 관계를 파악할 수 있음을 시사한다.

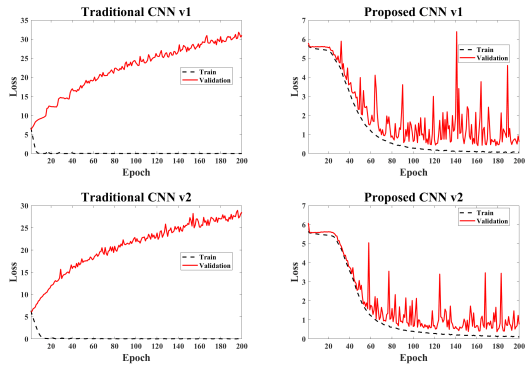


Fig. 5. Losses of the Traditional CNN and the Proposed CNN (first byte, $d=6$)

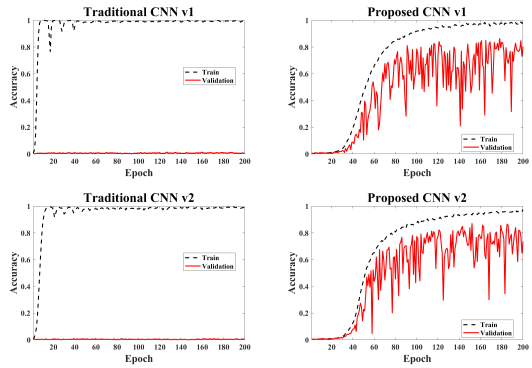
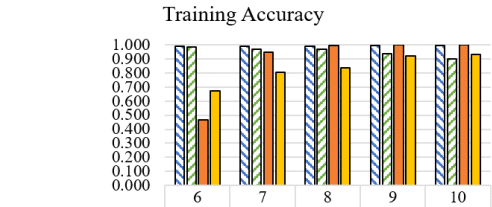
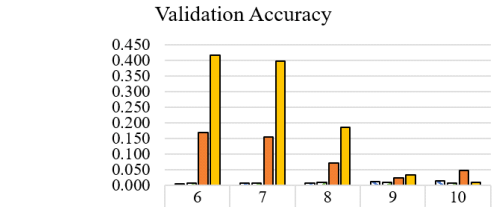


Fig. 6. Accuracies of the Traditional CNN and the Proposed CNN (first byte, $d=6$)

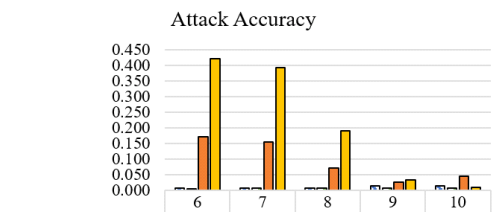
신경망의 깊이를 달리하여 16바이트 각각에 대해 학습 및 분석을 수행했을 때 정확도의 평균이 Fig. 7.과 같다. 전통적인 CNN은 학습 데이터 집합에 대한 정확도가 모두 1에 수렴하지만, 검증 데이터 집합과 공격 데이터 집합에 대한 정확도는 0.02이하로 매우 낮은 것을 볼 수 있다. 전통적인 구조는 신경망의 깊이가 얕은 경우 마지막 완전연결 층이 데이터의 이동을 감내하지 못하고, 깊은 경우 과적합이 발생하여 학습을 제대로 수행하지 못한다. 따라서 전통적인 구



	6	7	8	9	10
Traditional CNN v1	0.993	0.993	0.991	0.994	0.994
Traditional CNN v2	0.986	0.970	0.971	0.941	0.899
Proposed CNN v1	0.469	0.949	0.994	0.999	1.000
Proposed CNN v2	0.674	0.806	0.839	0.923	0.932



	6	7	8	9	10
Traditional CNN v1	0.006	0.007	0.008	0.012	0.014
Traditional CNN v2	0.007	0.008	0.009	0.009	0.008
Proposed CNN v1	0.170	0.154	0.071	0.025	0.047
Proposed CNN v2	0.417	0.398	0.185	0.034	0.010



	6	7	8	9	10
Traditional CNN v1	0.007	0.008	0.008	0.014	0.015
Traditional CNN v2	0.006	0.007	0.008	0.009	0.008
Proposed CNN v1	0.171	0.156	0.071	0.026	0.046
Proposed CNN v2	0.421	0.394	0.191	0.034	0.010

Fig. 7. Average accuracies of 16 bytes

조를 사용하는 경우 지터를 감내할 수 있도록 신경망을 깊게 구성하면서 과적합이 발생하지 않도록 충분히 많은 데이터를 확보해야 한다. 제안한 CNN은 신경망의 깊이가 깊어질수록 학습 데이터 집합에 대한 정확도는 높아지나, 검증 및 공격 데이터 집합에 대한 정확도는 낮아지는 양상을 보인다. 이는 신경망이 깊어지면 용량이 너무 커져 과적합이 발생했기 때문이다. 즉, 신경망의 깊이가 얕더라도 검증 및 공격 데이터 집합에 대한 정확도가 높은 것은 신경망의 지터에 대한 강건성이 은닉층의 구조에 의해 나타나는 것이 아니라, 태생적인 구조 때문임을 시사한다. 따라서 제안한 구조는 신경망의 구조를 자유롭게 구성할 수 있으므로 신경망의 깊이가 깊도록 강요받지 않고 일반화 성능이 높은 신경망을 설계할 수 있다.

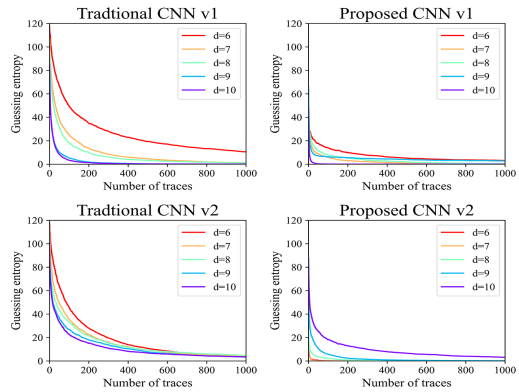


Fig. 8. Average guessing entropies of 16 bytes

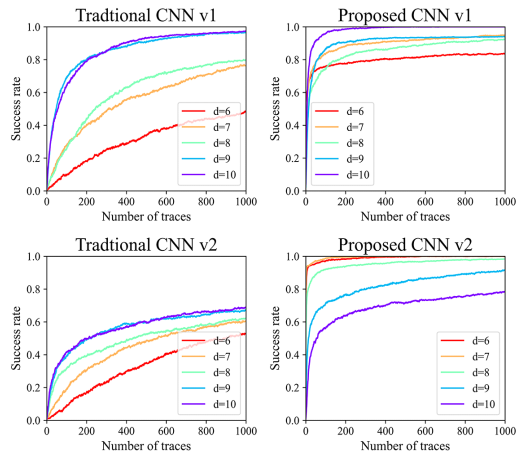


Fig. 9. Average guessing entropies of 16 bytes

학습된 신경망을 이용해 16바이트 각각에 대해 100번씩 분석을 수행한 결과 추측 엔트로피와 성공률의 평균이 각각 Fig. 8., Fig. 9.와 같다. 동일한 은닉층을 갖는 신경망끼리의 실험 결과를 비교했을 때, 과적합이 발생한 경우를 제외하면 제안한 신경망의 추측 엔트로피가 전통적인 신경망보다 낮았다. 특히 추측 엔트로피를 1미만으로 낮추기 위해 제안한 구조는 최적의 경우(v2, $d=7$) 18개의 데이터면 충분했지만, 전통적인 구조는 최적의 경우(v1, $d=10$)에도 223개의 데이터가 필요했다. 성공률 역시 제안한 구조가 전통적인 구조보다 높았으며, 90%이상의 성공률을 얻기 위한 데이터 수가 제안한 구조는 4인 반면, 전통적인 구조는 391로 매우 컸다. 따라서 제안한 구조를 사용하면 지터가 적용된 파형을 전통적인 구조에 비해 적은 데이터로 분석할 수 있다.

V. 결 론

본 논문에서는 전통적인 CNN 구조에서 완전연결 층 대신 GAP를 사용하면 지터에 강건한 신경망을 구성할 수 있음을 보였다. GAP를 사용하면 신경망의 모든 계층이 가중치를 공유하도록 구성할 수 있으므로 이동에 민감한 완전연결 층의 문제를 완화할 수 있다.

이를 ChipWhisperer-Lite 전력수집 보드에서 수집한 파형에 대해 실험한 결과 전통적인 CNN 구조는 검증 데이터 집합에 대한 정확도가 최대 1.4%에 불과했으나, 제안한 CNN 구조는 최대 41.7%로 높음을 확인했다. 이는 제안한 구조를 사용하면 과적합을 방지하면서 지터에 강건한 신경망 구조를 설계할 수 있음을 의미한다.

References

[1] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," Cryptographic Hardware and Embedded Systems, CHES 2002, LNCS 2523, pp. 13-28, Aug. 2002.

[2] W. Shindler, K. Lemke, and C. Paar, "A stochastic model for differential side channel cryptanalysis," Cryptographic Hardware and Embedded Systems, CHES 2005, LNCS 3659, pp. 30-46, Aug. 2005.

[3] G. Hospodar, B. Gierlichs, E. D. Mulder, I. Verbaushede, and J. Vandewalle, "Machine learning in side-channel analysis: a first study," Journal of Cryptographic Engineering, pp. 293-302, Oct. 2011.

[4] L. Lerman, R. Poussier, G. Bontempi, O. Markowitch, and F. X. Standaert, "Template attacks versus machine learning revisited and the curse of dimensionality in side-channel analysis," Journal of Cryptographic Engineering, pp. 301-313, Apr. 2017.

[5] L. Lerman, G. Bontempi, and O. Markowitch, "A machine learning approach against a masked AES," Journal of Cryptographic Engineering, pp. 123-139, Jun. 2015.

[6] K. Hornik, M. Stinchcombe, and H. White, "Multilayer feedforward networks are universal approximators," Neural Networks, pp. 359-366, Mar. 1989.

[7] F. Rosenblatt, Principles of neurodynamics: perceptrons and the theory of brain mechanisms, Spartan books, Mar. 1961.

[8] Y. Lecun, L. Bottou, Y. Bengio and P. Haffner, "Gradient-based learning applied to document recognition," in Proceedings of the IEEE, vol. 86, no. 11, pp. 2278-2324, Nov. 1998.

[9] L. Wouters, V. Arribas, B. Gierlichs, and Bart Preneel, "Revisiting a methodology for efficient CNN architectures in profiling attacks," Transactions on Cryptographic Hardware and Embedded Systems, TCHES, pp. 147-168, Jun. 2020.

[10] J. Kim, S. Kim, J. Woo, S. Park, and D. Han, "Deep learning-based side-channel analysis method with resistance to jitter," Korea Information Processing Society Conference, pp. 180-183, May. 2020.

[11] M. Lin, Q. Chen, and S. Yan, "Network In Network," 2nd International Conference on Learning Representations, ICLR, Jul. 2014.

[12] F. Standaert, T. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," Advanced in Cryptology, EUROCRYPT'09, LNCS 5479, pp. 443-461, Apr. 2009.

[13] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray Jr., "Advanced Encryption Standard (AES)," NIST FIPS 197, Nov. 2001.

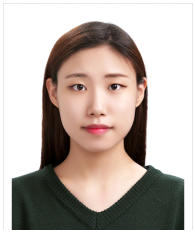
[14] D. Kingma and J. Ba, "Adam: a

method for stochastic optimization," 3rd International Conference on Learning Representations (ICLR), May. 2015.

〈저자소개〉

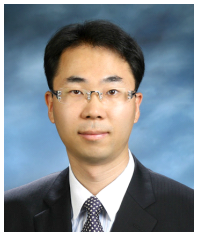
김 주 환 (Ju-Hwan Kim) 학생회원
2016년 3월~현재: 국민대학교 수학과 학사과정
〈관심분야〉 부채널 분석 및 대응법 설계, 딥러닝, 오류 주입 공격

우 지 은 (Ji-Eun Woo) 학생회원
2017년 3월~현재: 국민대학교 정보보안암호수학과 학사과정
〈관심분야〉 부채널 분석 및 대응법 설계, 머신러닝



박 소 연 (So-Yeon Park) 학생회원
2017년 3월~현재: 국민대학교 정보보안암호수학과 학사과정
〈관심분야〉 부채널 분석 및 대응법 설계, 머신러닝

김 수 진 (Soo-Jin Kim) 학생회원
2016년 3월~현재: 국민대학교 정보보안암호수학과 학사과정
〈관심분야〉 부채널 분석 및 대응법 설계, 대칭키 암호 알고리즘



한 동 국 (Dong-Guk Han) 종신회원
1999년 2월: 고려대학교 수학과 학사
2002년 2월: 고려대학교 수학과 이학석사
2005년 2월: 고려대학교 정보보호대학원 공학박사
2004년 4월~2005년 4월: 일본 Kyushu Univ., 방문연구원
2005년 4월~2006년 4월: 일본 Future Univ.-Hakodate, Post.Doc.
2006년 6월~2009년 2월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재: 국민대학교 정보보안암호수학과 정교수
〈관심분야〉 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석 및 대응법 설계, IoT 정보보호 기술