Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.5, Oct. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.5.987

이종 디바이스 환경에 효과적인 신규 딥러닝 기반 프로파일링 부채널 분석*

우 지 은,[1†] 한 동 국[2‡]
[1,2]국민대학교 (대학원생, 교수)

Novel Deep Learning-Based Profiling Side-Channel Analysis on the Different-Device*

Ji-Eun Woo,[1†] Dong-Guk Han[2‡]
[1,2]Kookmin University (Graduate student, Professor)

요 약

딥러닝 기반 프로파일링 부채널 분석은 사전에 소비전력과 같은 부채널 정보와 중간값과의 관계를 신경망이 학습한 뒤, 학습된 신경망을 이용하여 공격 파형의 비밀키를 찾아내는 기법이다. 최근에는 실제 부채널 분석 환경을 고려하기 위하여 교차 디바이스 환경에서의 분석 방안들이 제안되고 있다. 그러나 이러한 환경은 프로파일링 디바이스와 공격 디바이스의 칩이 다르면 공격 성능이 낮아지는 한계점이 존재한다. 따라서 본 논문에서는 공격자가 프로파일링 디바이스와 다른 칩을 가지는 공격 디바이스를 가지고 있는 환경을 이종 디바이스라고 정의하고, 이러한 환경을 고려한 분석 방안을 제안하고자 한다. 프로파일링 데이터와 공격 데이터에서 발생하는 도메인 차이를 줄이기 위해 비지도 도메인 적응을 사용하였다. 또한, 각 데이터의 특징을 잘 추출하기 위하여 여러 전처리 데이터와 원본 데이터를 학습하는 신경망 구조인 MCNN를 이용하였다. 이종 디바이스 환경을 구성하기 위해 8-bit 기반 프로세서 1개, 32-bit 기반 프로세서 5개를 이용하여 AES-128 전력 파형을 수집하였다. 제안한 방법론을 적용한 신경망과 적용하지 않은 신경망의 공격 성능을 비교했을 때, 제안한 방법론을 적용한 신경망의 최소 분석 파형 수가 최대 25배 이상 낮아졌다.

ABSTRACT

Deep learning-based profiling side-channel analysis has been many proposed. Deep learning-based profiling analysis is a technique that trains the relationship between the side-channel information and the intermediate values to the neural network, then finds the secret key of the attack device using the trained neural network. Recently, cross-device profiling side channel analysis was proposed to consider the realistic deep learning-based profiling side channel analysis scenarios. However, it has a limitation in that attack performance is lowered if the profiling device and the attack device have not the same chips. In this paper, an environment in which the profiling device and the attack device have not the same chips is defined as the different-device, and a novel deep learning-based profiling side-channel analysis on different-device is proposed. Also, MCNN is used to well extract the characteristic of each data. We experimented with the six different boards to verify the attack performance of the proposed method; as a result, when the proposed method was used, the minimum number of attack traces was reduced by up to 25 times compared to without the proposed method.

Keywords: Side-channel analysis, Deep-learning, Profiling analysis, Unsupervised domain adaptation

Received(08. 17. 2022), Modified(09. 27. 2022), Accepted(09. 27. 2022)

* 본 연구는 고려대 암호기술 특화연구센터(UD210027XD)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

† 주저자, dnwldms928@kookmin.ac.kr
‡ 교신저자, christa@kookmin.ac.kr(Corresponding author)

I. 서 론

부채널 분석(side-channel analysis)이란 디바이스가 동작할 때 얻을 수 있는 부채널 정보인 전자파, 소리, 소비전력 등을 이용하여 디바이스의 비밀정보를 도출해내는 공격 방법이다[1]. 이때, 소비전력을 이용한 부채널 분석은 크게 프로파일링 부채널 분석(profiling side-channel analysis)과 비프로파일링 부채널 분석(non-profiling side-channel analysis)으로 나뉜다. 프로파일링 부채널 분석은 공격자가 공격 디바이스와 동일한 프로파일링 디바이스를 가지고 있다는 공격자 가정을 가진다. 소비전력과 그의 중간값과의 관계를 수학적 모델링을 통해 사전에 프로파일링하여 공격하는 기법이며, 대표적으로 템플릿 공격(template attack)[2]이 있다. 이러한 전통적인 프로파일링 부채널 분석은 공격자가 전력 파형에서 중간값과 관련이 있는 구간(point of interest) 선정이나 전처리를 어떻게 하느냐에 따라 공격 성능이 크게 좌우되는 효과를 가져오게 된다. 이러한 공격자 능력에 따른 문제점을 완화하기 위하여 딥러닝을 부채널 분석에 접목한 연구들이 제안되었다[3, 4, 5]. 딥러닝 기반 프로파일링 부채널 분석은 프로파일링 디바이스를 이용하여 신경망을 학습시키고, 이러한 신경망으로 공격 파형에서의 비밀키를 예측하는 공격법이다. 신경망은 스스로 중간값과 소비전력과의 관계에 적합한 관계식을 찾아내서 학습을 진행한다.

또한, 실제 부채널 분석 환경을 고려한 딥러닝 기반 프로파일링 부채널 분석 연구가 제안되었다[6]. 이러한 환경을 교차 디바이스 환경이라고 하며, 프로파일링 디바이스와 공격 디바이스가 동일한 종류의 칩을 사용하지만 서로 다른 디바이스인 경우를 일컫는다. 최근에는 프로파일링 디바이스에서 얻은 학습 파형과 공격 디바이스에서 얻은 공격 파형과의 도메인 차이를 줄이기 위해 비지도 도메인 적응을 이용한 교차 디바이스 환경에서의 공격법이 제안되었다[7].

본 논문에서는 교차 디바이스 환경에서 더 나아가 프로파일링 디바이스와 공격 디바이스가 다른 종류의 칩을 사용하는 환경을 이종 디바이스라고 정의하고, 이를 고려한 부채널 분석 방안을 제안한다. 또한, 8비트 프로세서인 Atmel XMEGA128과 32비트 프로세서인 STM32F0, STM32F1, STM32F3, STM32F4, SCARF-IoT를 이용하여 제안한 방안이 효과적임을 보인다.

Contribution: 프로파일링 디바이스와 공격 디바이스의 칩 종류가 동일하지 않아도 비지도 도메인 적응을 이용하여 공격 디바이스에서의 공격 성능을 좋게 하는 딥러닝 기반 프로파일링 부채널 분석 방안을 제안한다. 실험 결과를 통해 공격하고자 하는 디바이스로 학습된 신경망이 아니더라도 공격 디바이스에서의 비지도 도메인 적응을 통해 효과적으로 공격할 수 있음을 보여준다. 이때, 하나의 데이터에 대해 다양한 특징 데이터를 학습하는 MCNN(Multi-scale Convolution Neural Network) 구조를 이용하여 신경망의 정확도를 높임으로써 공격 성능을 더욱 높이고자 하였다.

II. 관련 연구

2.1 딥러닝 기반 프로파일링 부채널 분석

딥러닝 기반 프로파일링 부채널 분석은 공격자가 공격 디바이스와 유사하고 완전히 제어할 수 있는 프로파일링 디바이스를 가진다고 가정한다. 이러한 기기를 이용하여 수집한 부채널 정보와 중간값과의 관계를 신경망이 학습하는 프로파일링 단계가 있고, 학습한 신경망을 이용하여 공격 대상 알고리즘의 비밀정보를 예측하는 공격 단계가 있다. 각 단계에 대한 자세한 설명은 아래와 같다.

1. 프로파일링 단계
   프로파일링 디바이스에서 임의의 평문과 키로 암호화할 때 얻은 다량의 파형을 입력값으로, 그때의 중간값을 라벨로 구성하여 신경망을 학습한다. 이때, 일반적으로 S-Box 결괏값을 중간값으로 사용하며, 학습데이터 일부를 신경망의 정확도를 검증하기 위하여 검증 데이터 집합으로 사용한다.
2. 공격 단계
   프로파일링 단계에서 학습한 신경망을 이용하여 공격 디바이스에서 고정된 키로 얻은 공격 파형에 대응되는 중간값을 예측하여 비밀키를 도출한다.

일반적으로 프로파일링 부채널 분석의 공격 성능 지표로는 게싱 엔트로피(guessing entropy)를 사용한다[8]. 게싱 엔트로피는 신경망이 예측한 확률 결과를 내림차순으로 정렬했을 때 옳은 키의 평균 순위이다. 이때, 옳은 키에서의 공격 파형 수에 따른 게싱 엔트로피가 0에 빠르게 수렴할수록 최소 분석 파형 수가 적어지므로 공격 성능이 좋다는 것을 의미한다.

2.2 역전파를 이용한 비지도 도메인 적응

도메인 적응(domain adaptation)은 학습데이터와 테스트 데이터와의 도메인 분포가 다르지만 동일한 과업(task)이 주어질 때 사용되는 방법론이다. 그중 비지도 도메인 적응(unsupervised domain adaptation)은 학습데이터의 라벨은 주고 테스트 데이터의 라벨은 주지 않았음에도 도메인 적응을 적용하여 과업을 수행할 수 있는 기술이다[9]. 이는 테스트 데이터가 학습데이터와는 다른 도메인이지만 도메인 차이를 줄여 학습데이터와 테스트 데이터와의 분포를 비슷하게 만들고 과업을 수행하도록 한다. 비지도 도메인 적응의 전체적인 구조는 Fig. 1.과 같다. 이때, X_s, X_t 는 각각 학습데이터와 테스트 데이터이다.

비지도 도메인 적응에서 사용하는 손실 함수는 분류 손실(classification loss)과 도메인 적응 손실(domain adaption loss)로 나뉜다. 분류 손실(l_{ds})은 학습데이터와 라벨을 이용하여 신경망의 분류 손실을 계산하고, 도메인 적응 손실(l_{dals})은 학습데이터 도메인 분포와 테스트 데이터 도메인 분포와의 차이를 계산한다. 따라서 신경망의 도메인 적응을 위해 사용하는 전체 손실 l은 수식 (1) 과 같다. 식에서 λ는 전체 손실에서 도메인 적응 손실의 비중을 조절하는 하이퍼 파라미터이다.

$$l = l_{ds} + \lambda \cdot l_{dals} \tag{1}$$

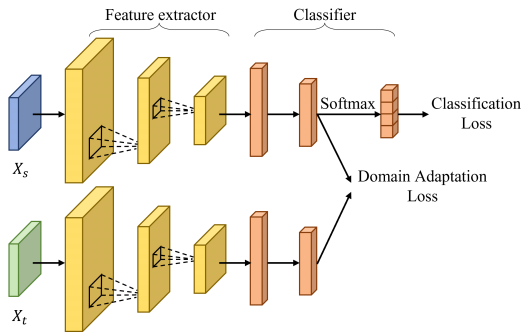


Fig. 1. An architecture for unsupervised domain adaptation (fine-tuning phase)

2.3 교차 디바이스 환경에서의 비지도 도메인 적응을 이용한 딥러닝 기반 프로파일링 부채널 분석

실제 환경에서는 프로파일링 디바이스와 공격 디바이스가 일치하지 않는 경우가 존재하기 때문에 이러한 교차 디바이스 환경에서의 프로파일링 부채널 분석에 관한 연구가 활발히 진행되고 있다. 그중에서도 공격자 가정을 더욱 완화하여 공격 파형의 라벨 없이도 비지도 도메인 적응을 이용해 공격 디바이스에서의 공격 성능을 높이는 방법이 제안되었다[7]. 제안된 공격법의 단계는 아래와 같다.

1. 사전 학습 단계
   2.1절의 프로파일링 단계와 동일하다.
2. Fine-tuning 단계
   Fig. 2.와 같이 학습 파형과 라벨이 없는 공격 파형을 이용하여 분류 손실과 도메인 적응 손실을 계산한다. 이때, MMD는 학습데이터와 공격 데이터의 도메인 차이를 줄일 때 일반적으로 사용하는 도메인 적응 손실 함수이고, X_s, X_t 는 각각 학습데이터와 테스트 데이터이다. 그 후 수식 (1)과 같이 전체 손실 l을 계산하여 신경망을 학습시킨다.
3. 공격 단계
   Fine-tuning한 신경망을 이용하여 공격 파형에 대응되는 중간값을 예측하여 비밀키를 도출한다.

8개의 Atmel XMEGA 128A1U (8-bit 기반 프로세서)를 이용하여 교차 디바이스 환경에서 실험을 진행하였고, Fine-Tuning을 하지 않은 신경망에 대해서 공격했을 때 대부분의 교차 디바이스에서 500개 이상의 공격 파형으로도 게싱 엔트로피가 0으

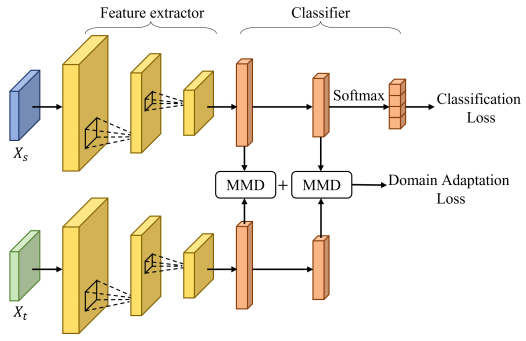


Fig. 2. An architecture for unsupervised domain adaptation on SCA (fine-tuning phase)

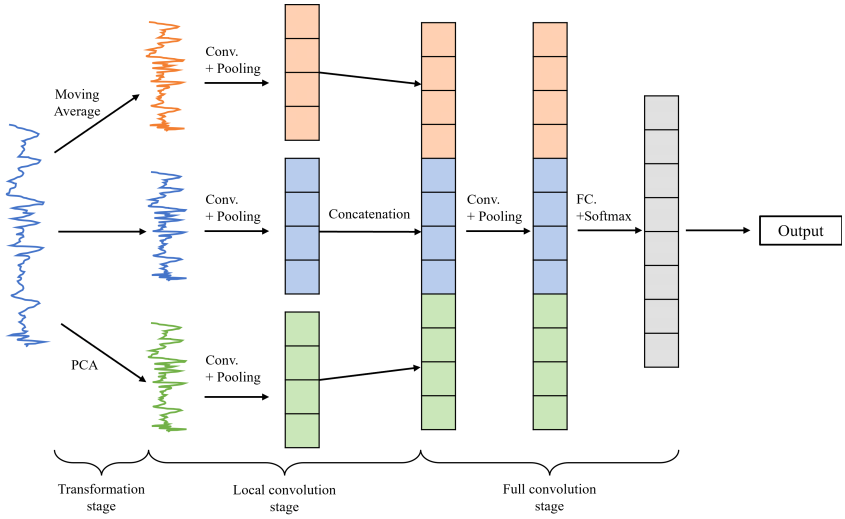


Fig. 3. MCNN architecture

로 수렴하지 않는 결과를 보였다. 그러나 Fine-Tuning을 진행하였을 때, 30개 이하의 공격 파형으로 모든 교차 디바이스에서 게싱 엔트로피가 0으로 수렴하는 결과를 보였다.

III. 이종 디바이스 환경에 효과적인 신규 딥러닝 기반 프로파일링 부채널 분석 방안

3.1 MCNN

MCNN(Multi-Scale Convolution Neural Network)은 Multi-branch 구조를 사용하는 신경망 구조로 데이터의 서로 다른 특징 공간을 추출하여 학습한다[10]. MCNN의 구조는 Fig. 3.과 같고, 크게 세 가지 구간으로 나뉜다.

1. Transformation stage
   입력 데이터에 대해서 여러 전처리 과정을 거치는 단계로 Moving average, PCA 등을 거쳐 서로 다른 특징 공간을 추출한다. 이렇게 생성한 데이터들과 원본 데이터를 Local convolution phase의 입력 데이터로 사용한다. 이때, 각 입력 데이터를 branch라고 한다.
2. Local convolution stage
   입력으로 들어온 branch에 대하여 콘볼루션 층을 이용해 특징을 추출한다. 이때, branch는 각각 콘볼루션 층을 가지고 있으므로 독립적으로 특징이 추출된다.
3. Full convolution stage
   앞선 단계에서 추출된 특징들을 연접하여 콘볼루션 층의 입력으로 사용한다. 이 단계에서의 구조는 일반적인 CNN 구조와 동일하며, 콘볼루션 층과 완전연결 층으로 이루어져 있다.

이 같은 MCNN 구조는 전통적인 CNN 구조보다 데이터에 대한 서로 다른 특징 공간을 입력으로 함으로써 입력 데이터에 대한 학습을 효과적으로 할 수 있도록 도와준다.

3.2 도메인 적응 손실 함수

최대 평균 불일치(Maximum Mean Discrepancy, MMD)[11]는 학습데이터와 테스트 데이터 특징 공간의 도메인 차이를 최소화할 때 일반적으로 사용되는 손실 함수이다. 자세한 손실 함수식은 아래의 수식 (2)와 같다.

$$MMD(X^s, X^t) = \frac{1}{n_s}\sum_{i=1}^{n_s}\phi(x_i^s) - \frac{1}{n_t}\sum_{j=1}^{n_t}\phi(x_i^t) \tag{2}$$

이때, ϕ는 원소를 재생적 커널 힐버트 공간(reproducting kernel hilbert space)으로 대응시켜주는 커널(kernel) 함수이다. X^t, X^s는 각각 학습 도메인, 테스트 도메인이며 n_t, n_s는 각각 학습데이터

의 수, 테스트 데이터를 나타낸다.

기존 논문[7]에서는 경험적인 근거를 토대로 MMD를 수식 (3)과 같이 정의하여 사용하였다.

$$\widehat{MMD}^2(X^s, X^t) = \frac{1}{n_s^2}\sum_{i=1}^{n_s}\sum_{j=1}^{n_s}\ker(x_i^s, x_j^s) + \frac{1}{n_t^2}\sum_{i=1}^{n_t}\sum_{j=1}^{n_t}\ker(x_i^t, x_j^t) - \frac{2}{n_s \cdot n_t}\sum_{i=1}^{n_s}\sum_{j=1}^{n_t}\ker(x_i^s, x_j^t) \quad (3)$$

이때,

$$\ker(\cdot) = \frac{1}{m}\sum_{j=1}^{m} k_j,\ k_j(x, x') = e^{-||x-x'||^2/\gamma}$$

이다.

본 논문에서는 기존 논문과 동일하게 수식(3)을 도메인 적응 손실 함수로 사용한다.

3.3 이종 디바이스 환경에서의 신경망 설계 및 분석 방안

본 절에서는 프로파일링 디바이스와 공격 디바이스가 다른 칩을 사용하는 이종 디바이스 환경에서의 효과적인 신경망 설계 및 분석 방안을 제안한다.

기존 연구[7]에서는 프로파일링 디바이스와 공격 디바이스가 칩 종류는 동일하나 디바이스 종류는 다른 환경을 다루었지만, 본 논문에서는 칩의 종류가 다른 이종 디바이스 환경을 다룬다. 따라서 공격하고자 하는 디바이스로 학습된 신경망이 아니더라도 공격 디바이스에서의 비지도 도메인 적응을 통해 적은 공격 파형 수로도 공격할 수 있음을 보여준다. 또한, MCNN을 이용해 신경망을 설계함으로써 각 데이터 도메인의 특징 공간을 서로 다른 전처리 과정을 통해 효과적으로 학습하고자 한다.

전처리 방식은 지터, 노이즈 등을 감내할 수 있는 Moving average와 주성분 분석을 사용하였다. Moving average는 5포인트씩 평균을 취한 값을 사용하였고, 주성분 분석을 이용하여 파형을 100포인트로 축소하였다. 이처럼 전처리 과정을 거친 데이터와 원본 데이터인 각 branch는 독립적이므로 신경망에서 서로 영향을 주지 않고 특징을 추출할 수 있다. 그 후 추출한 특징들을 연접하고 CNN 구조를 통과하여 특징을 추출한다. 이러한 과정을 학습데이터와 공격 데이터에 모두 적용하여 특징을 추출하고, 두 데이터에 대한 특징 공간의 도메인 차이를 도메인 적응을 이용해 줄임으로써 공격 디바이스로 프로파일링하지 않아도 공격 성능을 높일 수 있다.

IV. 실험 결과

본 절에서는 제안한 방법론의 공격 성능을 보이기 위해 프로파일링 데이터 집합으로만 학습한 신경망(pre-trained model)과 제안한 방법론을 적용한 신경망(MMD model)의 공격 파형 수에 따른 게싱 엔트로피를 비교한다.

4.1 실험 환경

제안한 방법론의 공격 성능을 확인하기 위해 서로 다른 디바이스에 대하여 총 6가지 데이터 집합을 구성하였다. 학습 파형은 임의의 평문과 키로 50,000번 암호화하여 전력 파형을 수집하였고, 그중 10%인 5,000개는 학습 과정에서 검증 데이터로 사용하였다. 공격 파형은 임의의 평문과 고정된 키로 10,000번 암호화하여 수집하였다. 자세한 실험 환경은 Table 1.과 같다. 본 논문에서는 AES-128의 첫 번

Table 1. Experimental environment

Dataset	Target chip	Capture board	Sampling rate
XMEGA128	8-bit MCU XMEGA128D4	ChipWhisperer-Lite[12]	29.538 MS/s
STM32F0	32-bit MCU STM32F071		
STM32F1	32-bit MCU STM32F100		
STM32F3	32-bit MCU STM32F303		
STM32F4	32-bit MCU STM32F405		
SCARF-IoT[13]	32-bit MCU STM32F412RGT	Lecroy Oscilloscope HDO610	500 MS/s

Table 2. Network structures for MCNN

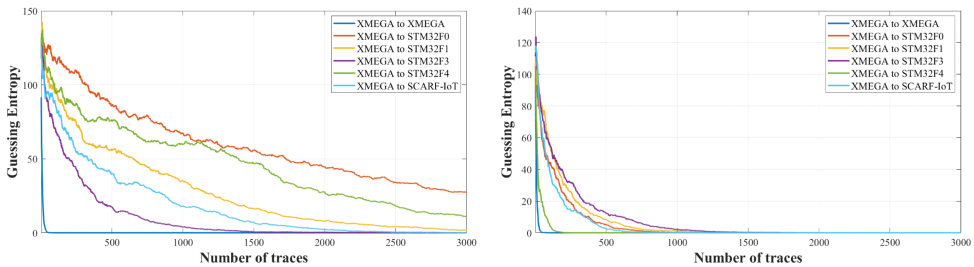
Trans-formation stage	Local convolution stage			Full convolution stage			FC layer			
	Filters	Kernel size	Pool size	Filters	Kernel size	Pool size				
Moving Average	(32, 64)	(1, 50)	(2, 50)	128	3	2	1024	512	256	9
Original	(32, 64)	(1, 50)	(2, 50)							
PCA	(32, 64)	(1, 1)	(2, 1)							

째 바이트 분석을 목표로 하므로 중간값(라벨)을 S-Box 결괏값으로 설정하였다. 또한, 본 논문에서 사용한 신경망 구조는 Table 2.과 같다. 최적화 알고리즘(optimizer)은 Adam[14], 학습률(learning rate)은 0.001, 배치 사이즈는 fine-tuning 시 데이터 수와 동일한 200으로 사용하였다.

4.2 실험 결과

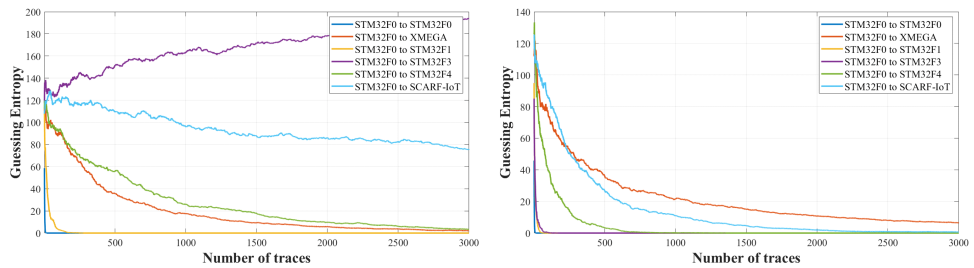
Fig .4., 5는 프로파일링 디바이스가 각각 XMEGA128, STM32F0이고 공격 디바이스별로 공격했을 때의 공격 파형 수에 따른 게싱 엔트로피를 도식화한 그래프이다. (a)는 프로파일링 데이터 집합으로만 학습한 신경망에서 공격했을 때 결과이고, (b)는 공격 데이터 집합을 이용해 제안한 방법론을 적용한 뒤 공격했을 때 결과이다. 각 그래프에서 x축은 게싱 엔트로피를 나타내며, y축은 공격 파형의 수를 나타낸다.

먼저 프로파일링 디바이스가 XMEGA128인 경우, Fig. 4. (a)와 (b)를 비교했을 때 (a)에서 게싱 엔트로피가 0으로 수렴하지 못했던 STM32F0, STM32F1, STM32F4가 (b)에서는 0으로 빠르게



(a) Pre-trained Model (b) MMD Model

Fig. 4. Experimental results when profiling device is XMEGA128
The guessing entropy of (a) pre-trained model, (b) MMD model



(a) Pre-trained Model (b) MMD Model

Fig. 5. Experimental results when profiling device is STM32F0
The guessing entropy of (a) pre-trained model, (b) MMD model

Table 3. The minimum number of attack traces

Profilind device	Attack device	Pre-trained model	MMD model
XMEGA128	XMEGA128	68	40
	STM32F0	＞3,000	1,000
	STM32F1	＞3,000	1,500
	STM32F3	2,400	1,600
	STM32F4	＞3,000	200
	SCARF-IoT	2,950	900
STM32F0	XMEGA128	＞3,000	＞3,000
	STM32F0	15	10
	STM32F1	250	58
	STM32F3	≫3,000	120
	STM32F4	＞3,000	890
	SCARF-IoT	≫3,000	2,900

수렴함을 볼 수 있다. 그뿐만 아니라 모든 공격 디바이스에서 게싱 엔트로피가 0으로 수렴하는 파형 수가 (a)에서보다 더 적어진 것을 볼 수 있다. 즉, 이는 최소 분석 파형 수가 더 낮아져 적은 파형 수로도 공격이 가능함을 의미한다. 프로파일링 디바이스가 STM32F0인 경우도 앞선 결과와 유사하게 대부분의 공격 디바이스에서 Fig. 5. (a)에서의 결과보다 (b)에서의 결과가 더 좋은 것을 볼 수 있다. Table 3.은 프로파일링 디바이스에 따라 각 모델의 최소 분석 파형 수를 나타낸 것이다.

따라서 프로파일링 디바이스와 공격 디바이스의 칩 종류가 다른 이종 디바이스 환경에서도 프로파일링 디바이스의 종류와 무관하게 제안한 방법론을 이용하면 공격 성능을 높일 수 있다.

V. 결 론

본 논문은 프로파일링 디바이스와 공격 디바이스가 다른 칩 종류를 가지는 환경인 이종 디바이스 환경에서 효과적인 딥러닝 기반 프로파일링 부채널 분석 방안을 제안하였다. 다양한 전처리 데이터와 원본 데이터를 이용하여 특징 공간을 추출하는 MCNN을 사용하였고, 이렇게 추출한 학습데이터의 특징 공간과 공격 데이터의 특징 공간 사이에서 발생하는 도메인 차이를 딥러닝 기술인 도메인 적응을 이용하여 줄이고자 하였다. 제안한 방법론을 사용하면 공격 디바이스에서 별도의 프로파일링 없이도 공격 성능을 높일 수 있다.

실제 공격 성능을 검증하기 위하여 총 6가지 디바이스에서 수집한 AES-128 파형을 이용하였다. 프로파일링을 각각 XMEGA128, STM32F0으로 수행하였을 때, 공격 디바이스 종류와 관계없이 제안한 방법론을 적용하면 공격 성능이 최대 25배 이상 높아진 것을 확인했다. 특히 XMEGA128의 경우, 노이즈가 심한 데이터인 STM32F4, SCARF-IoT으로 공격을 했을 때 각각 약 15배, 3배 이상 성능이 좋아졌음을 알 수 있다. 이는 신경망 구조를 MCNN을 이용함으로써 원본 데이터뿐만 아니라 Moving average, 주성분 분석과 같은 전처리 과정을 통해 데이터의 특징을 효과적으로 추출하여 동시에 학습하기 때문이다. 또한, 프로파일링 디바이스와 공격 디바이스의 조합에 따라 공격 성능이 달라지는 결과가 나타나는데, 이는 각 데이터에서 사용한 MCU 특성에 따라 신경망의 공격 성능에 영향을 끼치는 것이라 판단하였다.

따라서 향후에는 다양한 프로파일링 디바이스에 대하여 실험을 진행하고, MCU 특성에 따라 공격 성능에 미치는 영향을 분석할 계획이다.

References

[1] P.C. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems.”, Advances in Cryptology, CRYPTO ’96, LNCS vol 1109, pp. 104-113, Jan. 2001

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

[3] S. Ghandali, S. Ghandali, and S. Tehranipoor, "Profiled power-analysis attacks by an efficient architectural extension of a CNN implementation.", Proceedings of the 2021 22nd International Symposium on Quality Electronic Design (ISQED), pp. 395-400, Apr. 2021

[4] S. Picek, I. P. Samiotis, J. Kim, A. Heuser, S. Bhasin, and A. Legay, "On the performance of convolutional neural networks for side-channel analysis," in International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE), LNSC 11348, pp. 157 - 176, Dec. 2018.

[5] R. Benadjila, E. Prouff, R. Strullu, E. Cagli, and C. Dumas, "Deep learning for side-channel analysis and introduction to ascad database," Journal of Cryptographic Engineering, vol. 10, no. 2, pp. 163 - 188, Jun. 2020.

[6] H. Yu, H. Shan, M. Panoff, and Y. Jin, "Cross-device profiled side-channel attacks using meta-transfer learning." Proceedings of the in 2021 58th ACM/IEEE Design Automation Conference (DAC), pp. 703-708, Dec. 2021.

[7] P. Cao, C. Zhang, X. Lu, and D. Gu, "Cross-device profiled side-channel attack with unsupervised domain adaptation.", IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2021, no. 4, pp. 27-56, Aug. 2021.

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

[9] Y. Ganin and V. Lempitsky, "Unsupervised domain adaptation by backpropagation.", Proceedings of the 32nd International Conference on Machine Learning, vol 37, pp.1180-1189, Jul. 2015.

[10] Y. Won, X. Hou, D. Jap, J. Breier, and S. Bhasin, "Back to the basics: Seamless integration of side-channel pre-processing in deep neural networks." IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3215-3227. Apr. 2021

[11] A. Gretton, A. A.J. Smola, J. Huang, M. Schmittfull, K.M. Borgwardt, and B. Schölkopf, "Covariate shift and local learning by distribution matching", Dataset Shift in Machine Learning, MIT Press, Cambridge, MA, USA, pp. 131-160, 2009

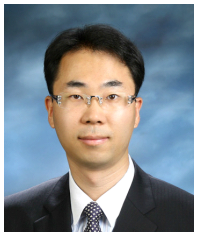
[12] CW1173 ChipWhisperer-Lite, "ChipWhisperer-Lite", https://wiki.newae.com/CW1173_ChipWhispererLite, Sep. 27, 2022

[13] Trusthingz, "trusthingz", https://trusthingz.org/, Sep. 27, 2022

[14] D. Kingma and J. Ba, "Adam: a method for stochastic optimization," 3rd International Conference on Learning Representations (ICLR), May. 2015.

〈저자소개〉

우 지 은 (Ji-Eun Woo) 학생회원
2021년 2월: 국민대학교 정보보안암호수학과 졸업
2021년 3월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 정보보호, 암호 분석, 부채널 분석, 딥러닝



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