Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.2, Apr. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.2.193

딥러닝 기반의 알려진 평문 공격을 통한 S-PRESENT 분석*

임 세 진,[1†] 김 현 지,[1] 장 경 배,[1] 강 예 준,[1] 김 원 웅,[1] 양 유 진,[1] 서 화 정[2‡]
[1,2]한성대학교 (대학원생, 교수)

S-PRESENT Cryptanalysis through Know-Plaintext Attack Based on Deep Learning*

Se-jin Lim,[1†] Hyun-Ji Kim,[1] Kyung-Bae Jang,[1] Yea-jun Kang,[1]
Won-Woong Kim,[1] Yu-Jin Yang,[1] Hwa-Jeong Seo[2‡]
[1,2]Hansung University (Graduate student, Professor)

요 약

암호 분석은 알려진 평문 공격, 차분 분석, 부채널 분석 등과 같이 다양한 기법으로 수행될 수 있다. 최근에는 딥러닝을 암호 분석에 적용하는 연구들이 제안되고 있다. 알려진 평문 공격(Known-plaintext Attack)은 알려진 평문과 암호문 쌍을 사용하여 키를 알아내는 암호 분석 기법이다. 본 논문에서는 딥러닝 기술을 사용하여 경량 블록 암호 PRESENT의 축소 버전인 S-PRESENT에 대해 알려진 평문 공격을 수행한다. 축소된 경량 블록 암호에 대해 수행된 최초의 딥러닝 기반의 알려진 평문 공격이라는 점에서 본 논문은 의의가 있다. 성능 향상 및 학습속도 개선을 위해 Skip connection, 1x1 Convolution과 같은 딥러닝 기법을 적용하였다. 암호 분석에는 MLP(Multi-Layer Perceptron)와 1D, 2D 합성곱 신경망 모델을 사용하여 최적화하였으며, 세 모델의 성능을 비교한다. 2D 합성곱 신경망에서 가장 높은 성능을 보였지만 일부 키공간까지만 공격이 가능했다. 이를 통해 MLP 모델과 합성곱 신경망을 통한 알려진 평문 공격은 공격 가능한 키 비트에 제한이 있음을 알 수 있다.

ABSTRACT

Cryptanalysis can be performed by various techniques such as known plaintext attack, differential attack, side-channel analysis, and the like. Recently, many studies have been conducted on cryptanalysis using deep learning. A known-plaintext attack is a technique that uses a known plaintext and ciphertext pair to find a key. In this paper, we use deep learning technology to perform a known-plaintext attack against S-PRESENT, a reduced version of the lightweight block cipher PRESENT. This paper is significant in that it is the first known-plaintext attack based on deep learning performed on a reduced lightweight block cipher. For cryptanalysis, MLP (Multi-Layer Perceptron) and 1D and 2D CNN(Convolutional Neural Network) models are used and optimized, and the performance of the three models is compared. It showed the

Received(01. 17. 2023), Modified(03. 08. 2023), Accepted(03. 08. 2023)
* 본 논문은 2022년도 한국정보보호학회 충청지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임
* This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2021-0-00540, Development of Fast Design and Implementation of Cryptographic Algorithms based on GPU/ASIC, 50%) and this work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%).
† 주저자, dlatpwls834@gmail.com
‡ 교신저자, hwajeong@hansung.ac.kr(Corresponding author)

highest performance in 2D convolutional neural networks, but it was possible to attack only up to some key spaces. From this, it can be seen that the known-plaintext attack through the MLP model and the convolutional neural network is limited in attackable key bits.

Keywords: Cryptanalysis, Know-plaintext Attack, S-PRESENT, Deep Learning, Convolutional Neural Network

I. 서 론

암호는 평문과 암호문 간의 상관관계를 없애는 혼돈(confusion)과 평문의 통계적 성질을 없애는 확산(diffusion)을 통해 키를 유추하거나 평문을 복원할 수 없도록 설계하는 것이 원칙이다[1]. 이러한 원칙에 기반하여 설계된 암호를 분석하는 연구가 활발하게 수행되고 있다. 암호 분석 기법에는 알려진 평문 공격, 차분 분석, 부채널 분석 등이 있다. 이 중 알려진 평문 공격은 공격자가 평문과 암호문을 알고 있다고 가정했을 때 평문, 암호문 쌍을 사용하여 비밀키를 알아내는 암호 분석 기법이다. 최근에는 딥러닝 기술을 암호 분석에 적용하는 연구들이 제안되고 있다. 본 논문에서는 저전력 환경에서 효율적인 구현이 가능하도록 설계된 경량 블록 암호 PRESENT의 축소 버전인 S-PRESENT에 대해 딥러닝 기술을 사용하여 알려진 평문 공격을 수행한다. 이는 축소된 경량 블록 암호에 대해 수행된 최초의 딥러닝 기반의 알려진 평문 공격이다. 암호 분석에는 MLP(Multi-Layer Perceptron)와 1D, 2D 합성곱 신경망 모델을 사용하여 최적화하고, 세 모델의 성능을 비교한다.

II. 관련 연구

2.1 선형 암호 분석(linear cryptanalysis)

선형 암호 분석은 1993년 Matsui가 제안한 강력한 암호 분석 방법이다[2]. 알려진 평문 공격이 선형 암호 분석에 해당되며, 암호 알고리즘 내부의 비선형 구조를 선형화하여 비밀키를 알아내는 방법이다.

2.2 합성곱 신경망(Convolutional Neural Network)

합성곱 신경망(CNN)은 이미지 처리에서 강력한 성능을 보이는 모델이다. 입력 데이터에서 필터를 통해 특징을 추출하고 강화하는 합성곱 계층과 추출된 특징을 기반으로 이미지를 분류하는 분류 계층으로 구성된다. 다른 신경망에 비해 훈련에 사용되는 매개변수의 수가 적기 때문에 학습 시간이 적게 걸린다는 장점이 있다. 합성곱 신경망 모델은 주로 2차원 이미지 특징 추출을 위해 2D 합성곱 연산이 사용되지만, 1차원 시퀀스 데이터에서 중요 정보를 추출하기 위해 1D 합성곱 연산이 사용되기도 한다. 2D 합성곱 연산에서는 커널이 수평 및 수직으로 이동하므로 이미지의 지역적 특징을 학습할 수 있으며, 1D 합성곱 연산에서는 커널이 한 방향으로 움직이므로 시계열 데이터를 학습할 수 있게 된다.

2.3 Skip connection[3]

Skip connection은 Residual Network[3]에서 제안된 기법으로 깊은 네트워크를 학습시키기 위한 방법 중 하나이다. Fig.1.과 같이 이전 층에서의 출력을 몇 개의 층을 건너뛴 후에 다음 층의 입력에 추가하여 추가적인 정보를 학습할 수 있도록 한다. 이 기법을 사용하면 기울기 소실 및 과적합을 방지할 수 있으며 더 쉽고 빠른 학습이 가능하다.

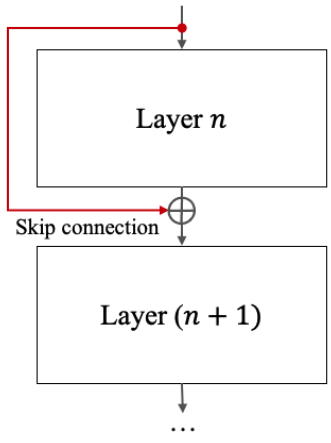


Fig. 1. Skip connection

2.4 1x1 Convolution[4]

구글은 2014년 ILSVRC(ImageNet Large

Scale Visual Recognition Challenge)[5]에서 연산량을 줄이기 위한 방법으로 1x1 Convolution을 적용한 GoogLeNet[4]으로 해당 대회에서 1등을 하였다. 연산 과정에서 1x1 Convolution 필터를 통과시킴으로써 채널의 수를 줄이게 되어 파라미터 수가 감소하게 된다. 파라미터 수가 적으면 연산량과 메모리 사용량 및 학습 시간을 줄일 수 있으며 과적합의 발생을 완화할 수 있다. 또한 계층 수를 늘리는데 상대적으로 부담이 적어 ReLU 활성화함수가 더 많이 적용될 수 있으므로 모델의 비선형성을 증가시킨다. 비선형성의 증가로 데이터의 복잡한 패턴을 보다 잘 학습하여 모델의 성능이 향상될 수 있다. 해당 대회에서 GoogLeNet의 계층 수가 가장 많았지만 1x1 Convolution을 사용하여 가장 적은 파라미터 수를 가질 수 있었다.

2.5 딥러닝을 사용한 블록 암호 분석 연구 동향

2.5.1 DL-Cryptanalysis of Lightweight Block Ciphers[6]

[6]은 MLP 기반 암호 분석 모델을 개발하여 S-DES8/10, SIMON32/64, SPECK32/64 블록 암호 알고리즘에 대해 알려진 평문 공격을 수행하였다. 평문과 암호문 쌍은 비트로 표현한 후 연접하여 입력 데이터로 사용하였고, 키는 암호에 따라 랜덤 비트키와 키공간을 64개의 ASCII 문자로 제한한 텍스트키를 사용하였다. 랜덤 비트키는 모든 비트에 대해 발생확률이 동일하지만 텍스트키는 제한된 키공간을 사용하므로 특정 비트로 발생확률이 치우쳐져있다. 따라서 랜덤 비트키보다 텍스트키를 예측하기 쉽다. 해당 논문에서는 성능 평가를 위한 지표로 각 비트에 대한 예측 정확도를 확률로 나타내는 BAP(Bit Accuracy Probability)를 사용하였다. S-DES의 경우 두가지 키 모두에서 전체 라운드에 대해 공격을 성공했다. SIMON과 SPECK의 경우에는 S-DES에 비해 평문과 키 비트가 각각 4배, 6.4배 길기 때문에 키공간을 제한한 텍스트키에서만 전체 라운드에 대해 공격을 성공하였다. 이를 통해 평문과 암호문이 길어질수록 키를 예측하는 것에 한계가 있음을 알 수 있다. 전체 라운드 수는 순서대로 2, 32, 22이며, 각 암호 분석에 사용된 데이터셋의 수는 순서대로 6만개, 150만개, 150만개이다.

2.5.2 Revisited[7]

[7]에서는 [6]의 MLP 모델에 여러 딥러닝 기법을 적용하여 S-DES에 대해 향상된 성능을 보였다. 적용한 딥러닝 기법은 Skip connection과 GLU(Gated Linear Unit)[8]를 사용하였다. GLU는 정보의 출입을 제어하는 역할을 한다. 입력된 값이 중요한 정보일 경우 Sigmoid 곱에서 값이 유지되고, 중요한 정보가 아닐 경우 값이 사라지게 된다. 따라서 보다 중요한 요소에 집중할 수 있으며 더 빠르고 안정적인 학습이 가능하도록 한다. 결과적으로 [6]의 작업에 비해 평균적으로 5.3% 더 높은 정확도를 달성하였고, 매개변수의 수는 93.16% 더 감소시켰다. 추가적으로 S-AES16/16에 대한 암호 분석도 수행하였다. S-DES와 동일한 키공간을 사용할 때 더 많은 매개변수를 요구하면서 낮은 정확도를 보인다. 이는 신경망이 S-DES보다 S-AES를 학습하기 어렵다는 것을 나타낸다. 각 암호 분석에 사용된 데이터셋의 수는 순서대로 10만개, 160만개이다.

2.6 PRESENT[9]

PRESENT는 2007년 CHES에서 Bodganov[9] 등이 제안한 AES 기반의 SPN (Substitution and Permutation Network) 구조의 초경량 블록 암호이다. 저전력 소모와 높은 칩 효율이 요구되는 IoT 기기에 적용할 수 있도록 설계된 암호이며, 블록 크기는 64-bit이고, 키 크기는 80-bit와 128-bit로 나뉜다. 아래 그림 2와 같이 동작하며 총 31라운드를 거쳐 암호문을 출력하도록 구성되어있다[10].

2.5장에서 살펴본 이전 연구에 따르면 딥러닝 기반의 알려진 평문 공격에는 많은 평문, 암호문 쌍이 필요하며, 이를 저장하기 위한 충분한 메모리가 필요하다는 한계점이 있다. PRESENT64/80의 경우 80-bit 키를 예측하기 위해서 필요한 데이터셋의 수가 기하급수적으로 증가하며, 평문 및 암호문 길이도 총 128-bit로 길어져 암호 분석을 수행하기 어렵다. 따라서 본 논문에서는 PRESENT의 블록 크기, 키 크기, 라운드 수를 8-bit, 16-bit, 3으로 축소시킨 S-PRESENT8/16[11]을 대상으로 암호 분석을 수행한다. 두 암호의 파라미터를 정리하면 아래 Table 1.과 같다.

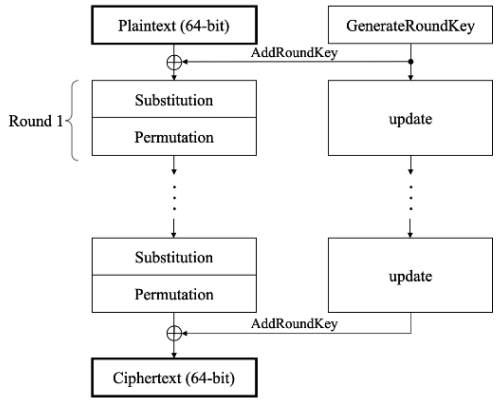


Fig. 2. Structure of PRESENT

Table 1. Parameters of PRESENT and S-PRESENT

	n-bit	k-bit	r
PRESENT-64/80	64	80	31
PRESENT-64/128	64	128	31
S-PRESENT-8/16	8	16	3

III. 딥러닝 기반의 알려진 평문 공격 제안

딥러닝을 사용하여 알려진 평문 공격을 수행하는 과정은 Fig. 3.와 같다. 먼저 대상 암호 알고리즘을 사용하여 모든 키의 경우의 수에 대해 랜덤 평문을 암호화하여 암호문을 생성한다. 데이터셋은 평문과 암호문을 연접한 쌍을 입력데이터로, 비밀키를 라벨로 사용한다. 본 논문에서 대상이 되는 S-PRESENT의 경우 입력 데이터와 출력 데이터는 각각 16-bit의 평문·암호문 쌍과 16-bit의 비밀키가 된다. 신경망 네트워크를 구성하여 입력 데이터에 대응하는 키를 예측한 후 실제 키와 비교하여 MSE 손실 함수를 통해 손실을 계산한다. 이후, 손실 값을 최소화하는 방향으로 학습을 진행하여 평문 및 암호문 쌍에 해당하는 올바른 키 값을 예측하도록 최적화한다. 이와 같은 과정을 통해 충분한 성능을 달성하도록 학습된 신경망의 가중치들은 고정되며, 추론 시에는 평문 및 암호문 쌍만을 가지고 키를 예측 할 수 있게 된다.

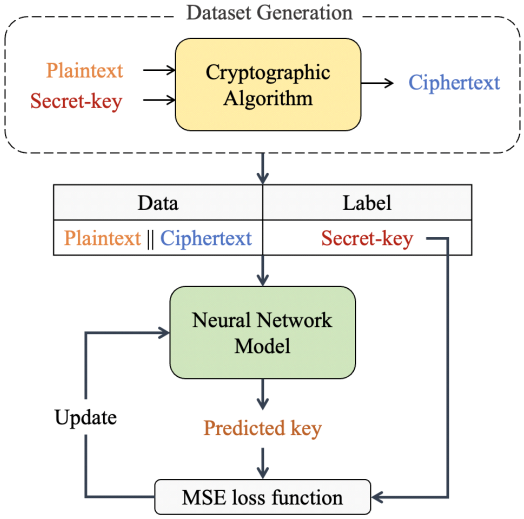


Fig. 3. System diagram for the proposed method

IV. 성능 평가 및 분석

4.1 실험 환경

본 실험을 위해 클라우드 기반 서비스인 Google Colaboratory Pro+를 활용하였다. Ubuntu 18.04.6 LTS 환경에서 13GB RAM과 Tesla T4 16GB GPU, 11.2버전의 Cuda, Python 3.8.16, Tensorflow 2.9.2이 사용되었다.

4.2 데이터셋

본 실험에서 사용된 데이터셋 생성 과정은 다음과 같다. [11]의 S-PRESENT 알고리즘을 통해 공격하고자하는 키 비트 공간의 모든 경우의 수에 대해 랜덤 평문을 암호화하여 암호문을 생성한다. 예를 들어 10-bit 키공간에 대해 공격을 수행한다면, 가능한 키 값의 경우의 수는 1024가지가 된다. 8-bit의 랜덤 평문에 대해 비밀키의 모든 경우의 수를 반영하여 암호문을 생성하고, 랜덤 평문과 암호문을 연접하여 입력데이터로 사용한다. 이때 암호화에 사용된 비밀키가 입력데이터에 대한 라벨이 된다. 한 키공간에 대해 총 1,024,000개의 데이터셋이 사용되었으며, 학습과 테스트에 사용된 데이터셋의 수는 각각 921,600개, 102,400개이다.

4.3 모델 구조

본 논문에서는 이전 연구[6-7]에서 데이터셋의 전

체적인 정보를 고려하기 위해 사용한 MLP 모델과 추가적으로 1D, 2D 합성곱 신경망 모델을 사용하여 알려진 평문 공격을 수행하였다. Fig. 4.는 본 논문에서 암호 분석에 사용된 2D 합성곱 신경망 모델의 구조를 나타낸다. 세가지 모델 모두 동일한 구조를 가지며, 1D 합성곱 신경망과 MLP 모델은 Conv2D층을 각각 Conv1D층과 Linear층으로 변경하면 된다. 데이터셋의 수가 많아 학습에 많은 시간이 소요되므로 빠른 학습을 위해 Skip connection 기법을 적용하였다. 또한 효율적인 학습을 위해 학습률을 점차 줄여가며 학습을 수행할 수 있도록 옵티마이저에 지수적 감쇠 방식을 적용하였다.

각 모델에 적용된 상세한 하이퍼파라미터 정보는 Table 2.와 같다. 각 모델에서 높은 성능을 나타내도록 최적화된 수치이다.

2D 합성곱 신경망의 경우 GoogLeNet의 1x1

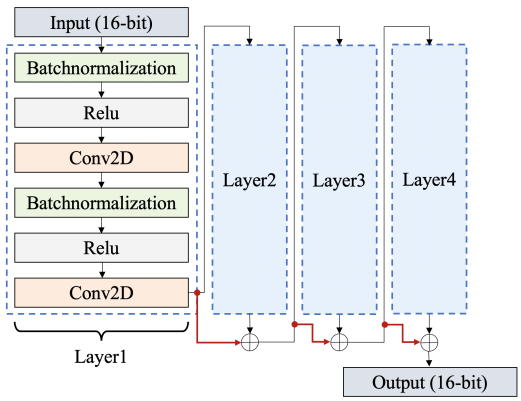


Fig. 4. Model Structure for S-PRESENT Cryptanalysis

Table 2. Hyperparameter details of the models

Hyperparameters	MLP	CNN1D	CNN2D
Kernel size	-	3	1
Batch size	128		
Loss function	MSE loss		
Activation funtion	ReLU		
Optimizer	Adam (Exponential decay method)		
Range of lr	0.001 ~ 0.1	0.001 ~ 0.01	0.001
Epochs	30		

Table 3. Comparing number of parameters in CNN2D

Kernel size	Total parameters
1	142,544
3	1,223,888

Convolution 기법을 적용하여 커널의 크기를 1로 설정하였다. Table 3.은 동일한 구조의 2D 합성곱 신경망 모델에서 커널 사이즈만 1과 3으로 설정했을 때의 파라미터 수를 보여준다. 1x1 Convolution 기법을 적용했을 때의 파라미터 수가 그렇지 않았을 때보다 약 8.6배 더 적은 것을 알 수 있다. 1x1 Convolution 기법은 2차원 데이터에서 효과적인 기법이므로 1차원 데이터를 대상으로 하는 1D 합성곱 신경망에 적용할 경우 파라미터 수에 변화가 없다. 1D 합성곱 신경망에서는 커널 사이즈를 3으로 했을 때 가장 높은 성능을 보여 3으로 설정하였다.

4.4 성능 평가

모델별 키 비트에 따른 자세한 실험 결과는 Table 4.에 정리하였다. 모든 비트에 대해 예측 정확도가 0.5를 초과해야 해당 키공간에서 공격이 성공한 것으로 간주한다. S-PRESENT의 전체 키공간인 16-bit에 대해서는 공격이 불가능하여 9-bit 키공간부터 한 비트씩 키공간을 늘려가며 각 모델이 공격할 수 있는 최대 키공간을 확인하였다. MLP, 1D, 2D 합성곱 신경망은 각각 12-bit, 11-bit, 13-bit 키공간까지 공격이 가능하였다. 키공간에 따른 세 모델의 분석 성능을 비교했을 때 2D 합성곱 신경망이 가장 좋은 성능을 보임을 알 수 있다. 이전 연구[6-7]에서는 전역적인 정보를 고려할 수 있는 MLP 모델을 사용하였지만, 본 실험의 결과를 통해 인접한 영역이 비슷한 특징을 갖는 지역적 특성도 있음을 알 수 있다. 본래 암호는 단일 비트가 변경되면 거의 모든 비트가 영향을 받기 때문에 지역적 특징을 갖기 어렵지만, 본 실험에서 사용한 S-PRESENT는 라운드 수가 축소된 암호였기 때문에 2D 합성곱 신경망에서 가장 좋은 성능을 보였을 것으로 예상된다. MLP 모델과 2D 합성곱 신경망의 성능 차이가 크게 나지 않았다는 점으로 미루어봤을 때 보편적인 암호 알고리즘 분석에 사용할 수 있는 모델은 데이터의 전체적인 정보를 고려할 수 있는 MLP 모델이다.

Table 4. BAP and Average of accuracy for models (9~13-bit key space)

Model	Key	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}	7^{th}	8^{th}	9^{th}	10^{th}	11^{th}	12^{th}	13^{th}	14^{th}	15^{th}	16^{th}	AVG
MLP	9-bit	1.0	1.0	1.0	1.0	1.0	1.0	1.0	0.64	0.65	0.66	0.67	0.63	0.61	0.66	0.61	0.57	0.79
	10-bit	1.0	1.0	1.0	1.0	1.0	1.0	0.62	0.62	0.63	0.63	0.63	0.61	0.6	0.54	0.6	0.59	0.75
	11-bit	1.0	1.0	1.0	1.0	1.0	0.56	0.58	0.56	0.56	0.56	0.57	0.54	0.52	0.55	0.54	0.53	0.69
	12-bit	1.0	1.0	1.0	1.0	0.51	0.53	0.56	0.53	0.54	0.53	0.54	0.51	0.51	0.52	0.52	0.51	0.64
CNN1	9-bit	1.0	1.0	1.0	1.0	1.0	1.0	1.0	0.71	0.72	0.71	0.73	0.71	0.7	0.7	0.69	0.68	0.83
	10-bit	1.0	1.0	1.0	1.0	1.0	1.0	0.63	0.63	0.64	0.64	0.64	0.62	0.61	0.56	0.61	0.59	0.76
	11-bit	1.0	1.0	1.0	1.0	1.0	0.56	0.58	0.56	0.57	0.56	0.57	0.55	0.53	0.55	0.55	0.53	0.69
CNN2	9-bit	1.0	1.0	1.0	1.0	1.0	1.0	1.0	0.71	0.71	0.71	0.71	0.69	0.69	0.67	0.68	0.66	0.83
	10-bit	1.0	1.0	1.0	1.0	1.0	1.0	0.62	0.62	0.63	0.63	0.63	0.61	0.61	0.57	0.6	0.58	0.76
	11-bit	1.0	1.0	1.0	1.0	1.0	0.57	0.59	0.57	0.58	0.58	0.58	0.56	0.55	0.55	0.56	0.54	0.7
	12-bit	1.0	1.0	1.0	1.0	0.52	0.54	0.56	0.53	0.54	0.54	0.54	0.52	0.51	0.52	0.52	0.52	0.65
	13-bit	1.0	1.0	1.0	0.54	0.51	0.52	0.55	0.52	0.52	0.53	0.53	0.51	0.51	0.51	0.51	0.51	0.61

Table 5.는 세 모델의 파라미터 수를 비교한 것이다. MLP와 2D 합성곱 신경망의 파라미터 수는 동일하지만 2D 합성곱 신경망의 더 높은 성능을 보이며, 더 빠른 학습이 가능하다. 따라서 S-PRESNET 알고리즘의 데이터셋에 대하여 2D 합성곱 신경망이 같은 수의 파라미터에서 더 양질의 특징을 추출하며 학습 시간도 적게 걸린다는 것을 알 수 있다. 키 비트별 예측 정확도에 따라 해당 비트의 안전성을 알 수 있다. 다른 키 비트에 비해 예측 정확도가 높은 키 비트일수록 비교적 예측이 쉬워 취약하다고 볼 수 있다. 본 논문의 결과는 전체 16-bit 키공간 중 최대 13-bit까지 공격을 수행할 수 있었기 때문에 1-bit부터 3-bit는 분석에서 제외하였다. 분석을 수행한 키공간에 대해 세 모델에서 공통적으로 정확도가 높게 나온 7, 10, 11-bit는 취약한 비트에 해당되며, 대부분의 경우에서 0.6 미만의 정확도를 보인 16-bit가 안전한 비트에 해당된다.

Table 5. Comparing number of parameters

Model	Total parameters
MLP	142,544
CNN1D	412,880
CNN2D	142,544

V. 결 론

본 논문에서는 MLP 모델과 1D, 2D 합성곱 신경망 모델을 사용하여 S-PRESENT 경량 블록 암호에 대해 알려진 평문 공격을 수행하고 성능을 비교하였다. 축소된 경량 블록 암호에 대한 최초의 딥러닝 기반의 알려진 평문 공격 수행이라는 점에서 본 논문은 의의가 있다. 결과적으로 1x1 Convolution 기법을 적용한 2D 합성곱 신경망 모델을 통해 전체 16-bit 키공간 중 13-bit 키공간까지 공격에 성공하였고, 안전한 비트와 취약한 비트를 확인하였다. 세 모델의 성능 비교를 통해 S-PRESENT 암호에 대해 제안한 2D 합성곱 신경망 구조가 적은 파라미터를 사용하면서도 양질의 특징을 추출하며, 더 적은 학습 시간이 걸림을 알 수 있었다. 본 논문에서 분석 대상으로 삼은 암호가 8-bit 평문에 16-bit 키를 가짐에도 불구하고 전체 키공간에 대해 알려진 평문 공격에 실패하였다. 데이터의 수를 늘릴수록 성능이 향상되지만, 학습 시간 및 메모리 용량 측면에서 한계가 있어 일정 수준 이상은 학습이 수행되지 않는다. 이를 통해 MLP 모델과 합성곱 신경망을 통한 알려진 평문 공격은 암호 분석이 가능한 키 비트에 제한이 있음을 알 수 있다. 향후 Transformer와 같은 최신 딥러닝 모델을 사용하여 알려진 평문 공격을 수행함으로써 한정된 수의 데이터셋 상에서도 양질의 특징을 추출할 수 있는지 실험하고자 한다.

References

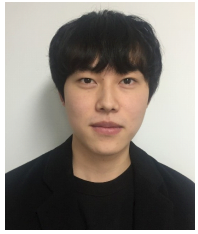
[1] C.E.Shannon, "Communication theory of secrecy systems," The Bell system technical journal, vol. 28, no. 4, pp. 656-715, Oct. 1949.

〔2〕 M.Matsui, "Linear cryptanalysis method for DES cipher," Lecture Notes in Computer Science, vol. 765, pp. 386 - 397, Jan. 1994.
〔3〕 K.He, X.Zhang, S.Ren, and J.Sun, "Deep residual learning for image recognition," Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 770 - 778, Jun. 2016.
〔4〕 C.Szegedy, W.Liu, Y.Jia, P.Sermanet, S.Reed, D.Anguelov, D.Erhan, V.Vanhoucke and A.Rabinovich, "Going deeper with convolutions," Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1-9, Oct. 2015.
〔5〕 O.Russakovsky, J.Deng, H.Su, J.Krause, S.Satheesh, S.Ma, Z.Huang, A.Karpathy, A.Khosla, M.Bernstein, A.C.Berg and L.F.Fei, "Imagenet large scale visual recognition challenge," International journal of computer vision, vol. 115, no. 3, pp. 211-252, Apr. 2015.
〔6〕 J.W.So, "Deep Learning-Based Cryptanalysis of Lightweight Block Ciphers," Security and Communication Networks, vol. 2020, pp. 1-11, Jul. 2020.
〔7〕 H.J.Kim, S.J.Lim, Y.J.Kang, W.W.Kim and H.J.Seo, "Deep Learning based Cryptanalysis of Lightweight Block Ciphers, Revisited," Cryptology ePrint Archive, Jul. 2022.
〔8〕 Y.N.Dauphin, A.Fan, M.Auli, and D. Grangier, "Language modeling with gated convolutional networks," International conference on machine learning, PMLR, vol. 70, pp. 933 - 941, Aug. 2017.
〔9〕 A.Bogdanov, L.R.Knudsen, G.Leander, C.Paar, A.Poschmann, M.J.B. Robshaw, Y.Seurin, and C.Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," Cryptographic Hardware and Embedded Systems, vol. 4727, pp. 450-466, Sep. 2007.
〔10〕 W.K.Park, G.P.Cebrián, S.J.Kim, K.H.Lee, D.W.Lim and K.S.Yu, "A Study on the Throughput Enhancement in Software Implementation of Ultra Light-Weight Cryptography PRESENT," The Journal of Korean Institute of Communications and Information Sciences, 42(2), pp. 316-322, Feb. 2017.
〔11〕 Github, "miniPresent python", https://github.com/xSAVIKx/PRESENT-cipher/blob/master/present/miniPresent.py, Sep. 05, 2022.

〈저 자 소 개〉

임 세 진 (Se-jin Lim) 학생회원
2022년 2월: 한성대학교 컴퓨터공학부 학사
2022년 3월~현재: 한성대학교 IT융합공학과 석사과정
〈관심분야〉 인공지능 보안, 양자 컴퓨터, 정보보안

김 현 지 (Hyun-Ji Kim) 학생회원
2020년 2월: 한성대학교 IT융합공학부 학사
2022년 2월: 한성대학교 IT융합공학과 석사
2022년 3월~현재: 한성대학교 정보컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 인공지능



장 경 배 (Kyung-Bae Jang) 학생회원
2019년 2월: 한성대학교 IT응용시스템공학과 학사
2021년 2월: 한성대학교 IT융합공학과 석사
2021년 3월~현재: 한성대학교 정보컴퓨터공학과 박사과정
〈관심분야〉 양자 컴퓨터, 정보보안

강 예 준 (Yea-jun Kang) 학생회원
2022년 2월: 한성대학교 컴퓨터공학부 학사
2022년 3월~현재: 한성대학교 IT융합공학과 석사과정
〈관심분야〉 블록체인, 인공지능 보안

김 원 웅 (Won-Woong Kim) 학생회원
2022년 2월: 한성대학교 컴퓨터공학부 학사
2022년 3월~현재: 한성대학교 IT융합공학과 석사과정
〈관심분야〉 블록체인, 인공지능 보안

양 유 진 (Yu-Jin Yang) 학생회원
2022년 2월: 한성대학교 IT융합공학부 학사
2022년 3월~현재: 한성대학교 IT융합공학과 석사과정
〈관심분야〉 양자 컴퓨터, 정보보안

서 화 정 (Hwa-Jeong Seo) 종신회원
2010년 2월: 부산대학교 컴퓨터공학과 학사
2012년 2월: 부산대학교 컴퓨터공학과 석사
2016년 1월: 부산대학교 컴퓨터공학과 박사
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~2023년 2월: 한성대학교 IT융합공학부 조교수
2023년 3월~현재: 한성대학교 융합보안학과 부교수
〈관심분야〉 암호구현