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.2023.33.2.175

PIPO 64/128에 대한 딥러닝 기반의 신경망 구별자*

김 현 지,[1†] 장 경 배,[1] 임 세 진,[1] 서 화 정[2‡]
[1,2]한성대학교 (대학원생, 교수)

Deep Learning-Based Neural Distinguisher for PIPO 64/128*

Hyun-Ji Kim,[1†] Kyung-Bae Jang,[1] Se-jin Lim,[1] Hwa-Jeong Seo[2‡]
[1,2]Hansung University (Graduate student, Professor)

요 약

차분 분석은 블록 암호에 대한 분석 기법 중 하나이며, 입력 차분에 대한 출력 차분이 높은 확률로 존재한다는 성질을 이용한다. 무작위 데이터와 특정 출력 차분을 갖는 데이터를 구별할 수 있다면, 차분분석에 대한 데이터 복잡도를 감소시킬 수 있다. 이를 위해 딥러닝 기반의 신경망 구별자에 대한 연구들이 다수 진행되었으며, 본 논문에서는 PIPO 64/128에 대한 최초의 딥러닝 기반의 신경망 구별자를 제안하였다. 여러 입력 차분들을 사용하여 실험한 결과, 0, 1, 3, 5-라운드의 차분 특성에 대한 3 라운드 신경망 구별자가 각각 0.71, 0.64, 0.62, 0.64의 정확도를 달성하였다. 이 구별자는 고전 구별자와 함께 사용될 경우 최대 8 라운드에 대한 구별 공격이 가능하도록 한다. 따라서 여러 라운드의 입력 차분을 처리할 수 있는 구별자를 찾아냄으로써 확장성을 확보하였다. 향후에는 성능 향상을 위한 최적의 신경망을 구성하기 위해 다양한 신경망 구조를 적용하고, 연관 키 차분을 사용하거나 다중 입력차분을 위한 신경망 구별자를 구현할 예정이다.

ABSTRACT

Differential cryptanalysis is one of the analysis techniques for block ciphers, and uses the property that the output difference with respect to the input difference exists with a high probability. If random data and differential data can be distinguished, data complexity for differential cryptanalysis can be reduced. For this, many studies on deep learning-based neural distinguisher have been conducted. In this paper, a deep learning-based neural distinguisher for PIPO 64/128 is proposed. As a result of experiments with various input differences, the 3-round neural distinguisher for the differential characteristics for 0, 1, 3, and 5-rounds achieved accuracies of 0.71, 0.64, 0.62, and 0.64, respectively. This work allows distinguishing attacks for up to 8 rounds when used with the classical distinguisher. Therefore, scalability was achieved by finding a distinguisher that could handle the differential of each round. To improve performance, we plan to apply various neural network structures to construct an optimal neural network, and implement a neural distinguisher that can use related key differential or process multiple input differences simultaneously.

Keywords: PIPO 64/128, Deep learning, Distinguisher, Differential cryptanalysis

Received(01. 10. 2023), Modified(03. 03. 2023), Accepted(03. 03. 2023)

* 본 논문은 2022년도 한국정보보호학회 영남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임.
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, 75%) and this work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 25%).

† 주저자, khj1594012@gmail.com
‡ 교신저자, hwajeong84@gmail.com(Corresponding author)

I. 서 론

차분 분석은 블록 암호에 대한 암호 분석 기법 중 하나이다. 암호 알고리즘이 안전하지 않게 설계된 경우, 입력 차분에 따른 출력 차분을 분석하여 키를 유추할 수 있도록 하는 기술이다. 차분 분석 특성을 활용한 인공 신경망 기반의 구별자를 사용하면 랜덤 데이터로부터 암호 데이터를 구별할 수 있게 되며, 차분 공격 시의 데이터 복잡도가 줄어들 수 있게 된다. 신경망 구별자에 대한 연구는 현재도 활발히 진행되고 있으며, 본 논문에서는 블록암호 PIPO 64/128에 대해 여러 라운드의 차분 특성을 고려한 최초의 신경망 구별자를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 인공 신경망 및 신경망 구별자에 대한 연구 동향을 살펴보고, 3장에서는 PIPO 64/128에 대한 신경망 구별자를 제안한다. 4장에서는 실험 및 성능 평가를 진행하고, 5장에서는 본 논문의 결론을 맺는다.

II. 관련 연구

2.1 인공 신경망[1]

인공 신경망은 데이터가 가진 특징을 학습함으로써 학습되지 않은 데이터가 입력될 경우에도 그에 대한 예측이 가능하도록 한다. 지도 학습, 비지도학습으로 나뉠 수 있으며, 기본적으로 여러 개의 노드로 이루어진 레이어가 여러 층 쌓인 구조를 갖는다. 즉, 입력 레이어와 출력 레이어 그리고 그 사이에 위치하는 은닉 레이어로 구성된다. 지도 학습을 위해서는 학습을 위한 데이터들이 입력되면 입력, 은닉, 출력 레이어를 거친 후 최종 예측 값이 출력된다. 각 레이어에서는 노드와 연결된 가중치와 입력 값끼리 연산을 수행한 후, 비선형 활성화 함수를 거친다. 이러한 과정을 통해 생성된 예측 값과 입력된 데이터가 갖는 실제 정답 값을 손실 함수에 입력한다. 손실 함수는 신경망의 성능 측정 지표이며, 손실이 적을수록 실제 값과 예측 값의 차이가 적다는 것을 의미한다. 따라서 손실 값을 최소화하기 위해 신경망의 가중치가 갱신되고, 갱신된 신경망에 다시 입력 데이터가 입력된다. 이러한 과정을 반복 수행하여 충분한 성능에 도달할 경우 학습을 종료한다. 학습된 신경망을 사용하여 실제로 추론을 수행할 경우, 신경망의 가중치는 모두 고정된 상태이며 학습에 사용되지 않은 시험 데이터들을 입력하여 예측 값을 얻어낼 수 있다. 인공 신경망에는 다양한 구조와 종류가 있다. 가장 기본적인 Multi Layer Perceptron (MLP)[2], 이미지 데이터 학습에 적합한 Convolution Neural Network (CNN)[3], 데이터 생성에 중점을 두는 생성형 신경망인 Generative Adversarial Network (GAN)[4] 등이 있으며, 해당 신경망을 사용하여 학습할 때 더 효율적이고 효과적인 학습을 위해 잔차 구조를 활용하는 ResNet[5] 등과 같이 다양한 기술이 존재한다.

2.2 인공 신경망 기반의 신경망 구별자

차분 분석은 블록암호에 대한 대표적인 암호 분석 방법[6]이며, 입력 차분과 출력 차분을 활용한다. 입력 차분은 두 개의 평문을 XOR한 값이고 출력 차분은 해당 평문 쌍을 암호화한 두 개의 암호문을 XOR한 값이다. 이상적인 암호 알고리즘은 입력 차분을 갖는 평문 쌍을 암호화했을 때 특정 출력 차분이 나오지 않고 랜덤한 분포를 얻는다. 그러나, 안전하지 않게 설계된 암호의 경우, 입력 차분을 갖는 평문 쌍을 암호화하면 특정 출력 차분을 갖게 된다. 차분분석은 이러한 성질을 이용하여 수행된다. 이 때, 랜덤 암호문과 차분을 갖는 암호문을 구별할 수 있다면, 차분 분석을 위한 데이터의 복잡도를 감소시킬 수 있다. 이러한 측면에서 인공지능은 좋은 솔루션으로 작용하며, 이에 대한 많은 연구들이 수행되고 있다.

Gohr[7]의 작업에서는 7-round speck32/64에 대해 최초의 신경망 구별자가 제안되었다. 앞서 언급하였듯이 무작위 데이터와 암호문 데이터를 특정 차분을 사용하여 분류할 수 있는 신경망을 설계하였으며, 해당 연구로부터 영감을 받아 많은 연구들이 수행되었다. 또한, Baksi et al. [8] 에서는 다중 입력 차분과 단일 차분을 고려한 두 가지의 새로운 신경망 구별자를 제안하였다.

[9]에서는 GIFT-COFB에 대한 입력 차분과 랜덤으로 생성한 입력 차분을 구별할 수 있는 GIFT-COFB에 대한 4라운드 신경망 구별자를 제안하였으며, 다양한 입력 차분에 대해 실험하였다.

[10]에서는 기존의 신경망 구별자가 갖는 메모리 문제 등을 해결하기 위해 고전 구별자와 신경망 구별자를 결합하였다. 즉, 고전 구별자에 0 라운드 입력 차분을 입력하여 n 라운드에 대한 출력 차분을 구하고, 해당 출력 차분을 신경망 구별자의 입력 차분으

로 사용하여 m라운드 구별자를 생성하여 $n+m$ 라운드에 대한 신경망 구별자를 제안하였다.

[11]에서는 Simon, Simeck에 대한 기본 신경망 구별자와 연관 키 신경망 구별자를 제안하였다. 연관 키 신경망 구별자는 암호화 시 사용되는 키도 차분을 가지는 경우이다. 해당 연구에서는 기본/연관 키 신경망 구별자에 대해 Simon32/64와 Simon64/128는 각각 12/15 라운드와 14/14 라운드를 달성하였고, Simeck32/64와 Simeck64/128에 대해 각각 12/15라운드와 18/22 라운드를 달성하였다. 이를 통해 연관 키 신경망 구별자를 사용할 경우 라운드 확장이 가능함을 볼 수 있다. 이처럼 현재 많은 연구들이 앞서 언급한 문제점을 극복하기 위한 다양한 시도를 하고 있으나, 한계점은 여전히 존재한다.

2.3 블록 암호 PIPO 64/128

ICISC'20에서 발표된 PIPO 블록암호는 8-bit AVR 환경에서 다른 64-bit 경량 블록암호를 능가하는 경량 블록암호이다[12]. 64비트 입출력과 128-bit (64/128) 및 256-bit (64/256) 키 크기를 가지며 SPN (Substitution Permutation Network) 구조로 설계되었으며, 64/128은 13 라운드, 64/256은 17 라운드이다. 비선형 S-box 연산을 수행하는 S-layer와 회전 연산을 수행하는 R-layer 및 키 덧셈으로 구성되어 있으며, 이러한 과정이 각 라운드마다 반복된다. S-layer의 경우 11개의 비선형 연산과 23개의 선형 비트 연산을 사용한 비트 슬라이싱 구현과 룩업 테이블을 이용한 구현이 있다.

III. 제안 기법

2장에서 살펴보았듯이 많은 딥러닝 기반의 신경망 구별자에 대한 연구들이 수행되고 있고, 블록암호 PIPO의 차분 특성을 찾기 위한 최신 연구 사례[13] 또한 존재한다. 해당 연구를 통해 높은 확률을 갖는 차분 특성이 발견되었으며, 이는 랜덤 데이터 분포에서 블록 암호를 구별해내는 구별자 공격에 더욱 효과적으로 활용될 수 있다. 그러나 PIPO에 대한 딥러닝 기반의 신경망 구별자는 제안되지 않았으므로, 본 논문에서는 국산 블록암호 PIPO64/128에 대한 최초의 딥러닝 기반의 신경망 구별자를 제시한다. 최근 제안된 PIPO 64/128의 여러 라운드의 차분 특성[13]들을 고려함으로써 고전 구별자와 함께 사용되어 더 많은 라운드에 대해 동작할 수 있도록 하였다.

3.1 데이터 셋

Fig. 1은 신경망 구별자의 학습을 위한 데이터 셋을 만들기 위한 과정을 보여준다. 특정 차분을 갖는 평문을 암호화 한 암호문 데이터와 랜덤 평문을 암호화 한 암호문 데이터를 생성한 후 데이터 셋을 구성하며, 세부 순서는 다음과 같다. 먼저, 독립적인 랜덤 평문 (P_0, P_1)을 선택한다. 차분을 만족하는 평문 쌍을 만들기 위해 P_0에 입력차분을 XOR한 평문인 P'_0를 구한다. 이후, 각 평문을 암호화하여 암호문 (C_0, C_1, C'_0)을 구한다. C_0과 C_1은 랜덤 평문 쌍을 암호화 한 암호문 쌍이므로 두 암호문을 연접하여 0으로 라벨링하고, C_0와 C'_0는 입력 차분을 만족하는 평문 쌍에 대한 암호문 쌍이므로 이를 연접하여 1으로 라벨링한다. 이러한 과정을 통해 생성된 데이터 셋은 Fig. 2와 같은 형식으로 구성된다.

Input: Input difference (δ), The number of data (N_{ds}), Encryption function (ENC)
Output: Dataset (DS)
for i=0 **to** $N_{ds}/2$ **do**
  Choose random plaintext $P_0, P_1 (P_1 \neq P_0 \oplus \delta)$
  $P'_0 = P_0 \oplus \delta$
  $C_0 = ENC(P_0)$, $C_1 = ENC(P_1)$, $C'_0 = ENC(P'_0)$
  $C_0 \,||\, C_1$ is labeled 0 (Random)
  $C_0 \,||\, C'_0$ is labeled 1 (Cipher)
  $DS \leftarrow C_0 \,||\, C_1$ and $C_0 \,||\, C'_0$
end for
return DS

Fig. 1. Dataset preparation

c_0			c'_0 or c_1		Label
0	1	⋯	1	1	0
⋮	⋮	⋮	⋮	⋮	⋮
1	0	⋯	0	1	1

DS

Fig. 2. Format of data set

3.2 모델 구성

Table 1은 PIPO에 대한 신경망 구별자의 하이퍼파라미터이다. 암호의 특성 상 각 비트가 모든 비트와 연관이 있으므로, 전역적인 정보를 반영하기에 효과적인 MLP 모델을 사용하였다 [14]. 이진분류 문제이므로 BCELoss 손실함수를 사용하였고, 과적합 방지를 위해 dropout 레이어를 사용하였다. 또한, 총 1000만 개의 데이터 셋을 사용하였으며, 실험을 통해 epoch의 수는 20으로 설정하였다.

Table 1. Hyperparameters of proposed neural distinguisher for PIPO 64/128

Epoch		20
Architecture		4 hidden layers with 128 units
The number of parameters		83969
Batch size		32
Activation		ReLu
Optimizer (Learning rate)		Adam (lr=0.001)
Loss function		BCELoss
Dropout		0.5
The number of data (1/2/3 round)	Training	7000/1750000/7000000
	Validation	2000/500000/2000000
	Test	1000/250000/1000000

3.3 학습 과정

Fig. 3은 학습 과정을 보여준다. Fig. 4와 같이 데이터를 입력 레이어에 입력한 후, 히든 레이어와 출력 레이어를 거쳐 모델의 최종 출력 값을 얻는다. 이후, 최종 출력 값과 데이터에 대한 실제 정답을 활용하여 BCELoss를 통해 손실을 구하고, 정확도를 계산한다. 해당 과정은 설정한 epoch의 수만큼 반복되면서 학습해나간다. 신경망 구별자는 이진분류를 수행하기 때문에 정확도가 0.5 이하인 경우에는 암호문과 랜덤 데이터를 구별할 수 없는 상태이므로 사용하지 않고, 반대로 정확도가 0.5보다 크다면 해당 모델은 암호문과 랜덤 데이터를 구별할 수 있는 것이므로 신경망 구별자로 사용될 수 있다. 따라서 훈련

Input: Dataset (DS), The number of hidden layer (h), The number of epoch ($EPOCH$)
Output: Trained model (M)
for epoch=1 **to** $EPOCH$ **do**
  $x \leftarrow Inputlayer(DS)$
  for $i = 1$ **to** h **do**
    $x \leftarrow Hiddenlayer(x)$
  $out \leftarrow Outputlayer(x)$
  Compute loss and accuracy (acc)
  Update parameters of neural network model
end for
If $acc \leq 0.5$ **then**
  Abort M
else if $acc > 0.5$ **then**
  return M

Fig. 3. Training process

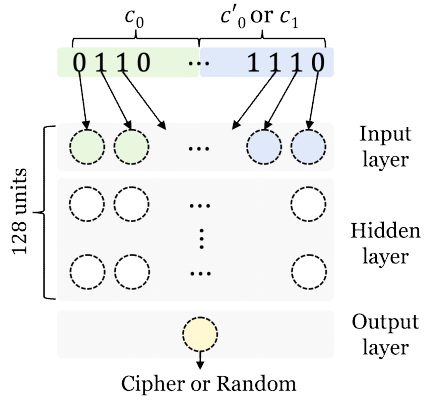

Fig. 4. Architecture of proposed method

된 모델을 사용하여 학습되지 않은 데이터에 대한 추론을 수행한다.

이러한 작업이 가능한 이유는 입력 데이터가 차분 특성을 가지며, 암호화를 반복하더라도 비선형 계층에 대한 차분의 전파는 확률적으로 예측 가능하기 때문이다. 즉, 특정 확률로 차분 특성이 존재하고, 이는 확률적으로 예측할 수 있으므로 딥러닝 기술을 통해 특정 입력 차분에 대한 출력 차분을 갖는 데이터임을 예측할 수 있는 것이다.

IV. 실험 및 평가

본 장에서는 제안 기법에 대한 실험을 진행하였으며, Apple M1 Pro 16GB RAM, Python

3.8.9, Pytorch 1.12.0 환경에서 수행되었다.

4.1 입력 차분

본 실험을 위해 [12]에서 제시된 입력 차분과 Table 2와 같이 [13]에서 제시된 입력 차분을 사용하였다. Table 2의 입력 차분들은 PIPO 64/128에 대해 자동화된 차분 특성 탐색 방법인 Mixed Integer Linear Programming (MILP)를 적용하여 얻은 결과이며, 각 라운드의 차분 특성이다.

Table 2. Input differential characteristics in [13]

Round	Input differential
0	0x0100010100010100
1	0x0000000000008000
2	0x0000000000080080
3	0x2011112000800080
4	0x404100408101c080
5	0x0000101000100000
6	0x0000000080000000
7	0x0001000004084000

4.2 실험 결과

Table 3은 PIPO 64/128에 대한 신경망 구별자의 실험 결과이다. 각 차분 특성들은 4.1절에 언급된 값이며, 본 실험의 결과는 모든 경우에 대해 5번씩 실험한 후 평균을 계산한 값이다. 또한, 사용된 1, 2, 3 라운드의 데이터의 수 (데이터 복잡도)는 각각 $2^{13.28771}$, $2^{21.25349}$, $2^{23.25349}$이다.

3 라운드 신경망 구별자에 대해 2, 3, 5, 7번 입력 차분은 각각 0.71, 0.64, 0.62, 0.64의 정확도를 달성하였으므로 본 실험을 통해 해당 차분들에 대한 3 라운드의 신경망 구별자가 검증된 것이다. 해당 입력 차분들은 각각 MILP로 구한 0 라운드, 1 라운드, 3 라운드, 5 라운드에 대한 차분 특성이며, 이들은 [15]에서 제시된 바와 같이 키 복구 공격을 위한 신경망 구별자로 사용될 수 있다. 다시 말하면, 제안된 신경망 구별자는 7번 차분 특성을 구별할 수 있으므로 5라운드 입력 차분에 대한 구별자로 동작 가능한 것을 의미한다. 3 라운드 신경망 구별자에 대해 20 epoch 보다 많이 학습할 경우, 정확도의 증가량이 감소하였다. 즉, 빠르게 수렴하므로 각 데이터들에 대해 20 epoch만으로도 충분히 학습될 수 있음을 확인하였다. 또한, 1 라운드에 대한 신경망 구별자의 경우 5 epoch만으로도 학습이 가능하였으며 3 라운드에 비해 더 간단한 데이터이므로 더 빠르게 수렴하는 것을 알 수 있다. 그리고, 각 라운드에 대한 결과를 비교해보면, 1, 2 라운드의 정확도는 큰 차이가 없으나 3 라운드의 경우 평균적으로 0.33의 정확도 손실이 발생하였다. 이처럼 각 입력 차분에 대해 동일한 신경망을 적용하면 입력 차분과 라운드 수에 따른 정확도 차이가 존재하였다. 따라서 라운드 및 입력 차분 특성에 맞는 최적의 신경망이 다를 것이며, 다양한 구조의 네트워크를 적용하여 더 높은 신뢰성을 갖는 신경망 구별자를 구성해야 할 것으로 생각된다.

4.3 PIPO 64/128에 대한 기존 구별자와의 비교

[12]에서는 차분/불능 차분 특성을 활용하여 6/4 라운드 고전 구별자를 제시하였다. 이는 본 논문에서 제안하는 신경망 구별자보다 각각 3/1 라운드만큼 더 높은 결과이다. 이러한 결과는 여러 딥러닝 기반의 구별자들이 갖는 메모리 사용량 문제로 인한 것으로 생각된다. 딥러닝은 많은 데이터를 기반으로 학습을 수행하며, 일반적으로 고차원 (복잡한) 데이터일수록 더 많은 데이터가 필요하다. Speck 32/64에 대한 7 라운드 신경망 구별자의 결과를 참고하면 $2^{23.25349}$의 데이터를 사용하였으며, 이보다 평문의 길이가 2배 긴 PIPO 64/128은 더 많은 데이터가 필요하게 된다. 실제로 본 실험에서 3 라운드와 동일하게 $2^{23.25349}$ 개의 데이터를 사용하여 4 라운드의 신경망 구별자를 동작시켜본 결과, 학습이 진행되지 않았으며, 이처럼 한 라운드만 증가하여도 정확도 손실이 발생하고 필요한 데이터의 수가 많아질 것임을 예상할 수 있다. 그러나, 본 실험이 수행된 환경의 제약으로 인해 $2^{23.25349}$개를 초과하는 64-bit 데이터를 사용하기 어려우므로 3 라운드 이상의 구별자를 얻을 수 없었다. 하지만 앞서 언급하였듯이 본 구현은 여러 라운드의 차분 특성에 대한 3 라운드 신경망 구별자이므로 [10]에서 제시된 바와 같이 고전 구별자와 신경망 구별자를 융합하면 최대 8 라운드에 대한 구별 공격으로 확장될 수 있다. 향후, 더 많은 라운드에 대한 공격을 위해서는 데이터의 차원을 축소시킬 수 있는 전처리 기술 등을 적용하여

Table 3. Result of proposed neural distinguisher for PIPO 64/128 (Tr, Val, Ts : Accuracy for training, validation and test data set)

Serial	Input difference	Round	Accuracy		
			Tr	Val	Ts
1	0x8800088008088000	1	1.00	1.00	1.00
		2	0.98	0.99	0.99
		3	0.50	0.50	0.50
2	0x0100010100010100	1	0.99	1.00	1.00
		2	0.99	0.99	0.99
		3	0.71	0.71	0.71
3	0x0000000000008000	1	0.99	1.00	0.99
		2	0.95	0.97	0.96
		3	0.63	0.64	0.64
4	0x0000000000080080	1	0.99	0.98	0.99
		2	0.98	0.99	0.99
		3	0.50	0.50	0.49
5	0x2011112000800080	1	0.99	0.99	0.99
		2	0.79	0.80	0.80
		3	0.61	0.62	0.62
6	0x404100408101c080	1	0.99	0.99	0.99
		2	0.73	0.74	0.74
		3	0.50	0.50	0.50
7	0x0000101000100000	1	0.99	0.99	0.99
		2	0.99	0.99	0.99
		3	0.63	0.64	0.64
8	0x0000000080000000	1	0.99	1.00	0.99
		2	0.99	0.99	0.99
		3	0.50	0.50	0.50
9	0x0001000004084000	1	0.99	0.99	0.99
		2	0.63	0.64	0.63
		3	0.50	0.50	0.50

메모리를 절약함으로써 더 많은 데이터를 사용할 수 있도록 해야 할 필요가 있다.

V. 결 론

최근 딥러닝 기술이 발전함에 따라 이를 활용한 암호 분석 연구들이 많이 수행되고 있다. 그 중, 구별자 공격은 블록 암호의 차분 특성을 활용하여 랜덤 데이터로부터 암호 데이터를 구별해내는 작업이므로 확률적인 예측이 가능하여 딥러닝 기술이 좋은 솔루션이 될 수 있으며 실제로 이에 관한 많은 연구들이 진행되었다. 그러나 국산 블록암호 PIPO에 대한 딥러닝 기반의 구별자 공격에 관한 연구는 아직 수행되지 않았다. 본 논문에서는 인공 신경망을 활용하여 여러 라운드의 입력 차분이 적용된 암호 데이터를 구별해 낼 수 있는 PIPO 64/128에 대한 최초의 신경망 구별자를 제시하였다.

실험 결과, MILP를 통해 구해진 입력 차분들에 대한 1~3 라운드의 신경망 구별자를 얻을 수 있었으며, 특히 0, 1, 3, 5 라운드의 차분 특성에 대해서는 3 라운드 신경망 구별자가 동작하였다. 이는 PIPO 64/128에 대한 6 라운드 고전 구별자보다 3 라운드 낮은 수치이며, 대상 암호인 PIPO 64/128이 64-bit의 평문을 가지므로 많은 특징을 갖는 고

차원의 데이터이며, 실험 환경의 제약으로 인해 충분한 양의 데이터를 사용할 수 없었기 때문으로 파악된다. 이러한 문제는 딥러닝 기반의 신경망 구별자가 갖는 고질적인 문제이다. 따라서 데이터의 복잡도를 낮출 수 있는 방안에 대한 연구가 필요할 것으로 생각된다.

그러나 제안된 신경망 구별자는 PIPO 64/128의 여러 라운드의 차분 특성들을 학습하였으며, 실제로 5 라운드 입력 차분에 대해 3 라운드 신경망 구별자가 동작하였다. 따라서 고전 구별자와 융합될 경우 최대 8라운드 키 복구 공격을 위해 활용될 수 있으며, 이로 인해 신경망 구별자가 갖는 라운드의 한계를 극복할 수 있을 것으로 기대된다. 이와 더불어 향후에는 연관 키 차분을 활용하거나 여러 입력 차분을 동시에 처리하는 신경망 구별자에 대한 연구 또한 진행할 예정이다.

References

[1] Haykin, Simon. "Neural networks and learning machines, 3/E," Pearson Education, Inc., Upper Saddle River, New Jersey 07458, pp. 1-906, 2009.

[2] Gardner, Matt W., and S. R. Dorling. "Artificial neural networks (the multilayer perceptron)—a review of applications in the atmospheric sciences," Atmospheric environment, Vol. 32, no. 14-15: pp. 2627-2636, Aug. 1998.

[3] Albawi, Saad, Tareq Abed Mohammed, and Saad Al-Zawi. "Understanding of a convolutional neural network," 2017 international conference on engineering and technology (ICET). pp. 1-6, Aug. 2017.

[4] Goodfellow, Ian, et al. "Generative adversarial networks," Communications of the ACM Vol. 63, no. 11: pp. 139-144, 2020.

[5] He, Kaiming, et al. "Deep residual learning for image recognition," Proceedings of the IEEE conference on computer vision and pattern recognition, Las Vegas, NV, USA, pp. 770-778, Jun. 2016.

[6] Heys, Howard M. "A tutorial on linear and differential cryptanalysis," Cryptologia, Vol. 26, no. 3: pp. 189-221, Jul. 2002.

[7] Gohr, Aron. "Improving attacks on round-reduced speck32/64 using deep learning," Annual International Cryptology Conference. Springer, Santa Barbara, CA, USA, pp.150-179, Aug. 2019.

[8] Baksi, Anubhab. "Machine learning-assisted differential distinguishers for lightweight ciphers," Classical and Physical Security of Symmetric Key Cryptographic Algorithms. Springer, Singapore, pp. 141-162, Jan. 2022.

[9] Rajan, Reshma, et al. "Deep Learning-Based Differential Distinguisher for Lightweight Cipher GIFT-COFB," Machine Intelligence and Smart Systems, Springer, Singapore, pp. 397-406, May. 2022.

[10] Yadav, Tarun, and Manoj Kumar. "Differential-ml distinguisher: Machine learning based generic extension for differential cryptanalysis," International Conference on Cryptology and Information Security in Latin America, Springer, Cham, Vol. 12912, pp. 191-212, Sep. 2021.

[11] LU, Jinyu, et al. "Improved (Related-key) Differential-based Neural Distinguishers for SIMON and SIMECK Block Ciphers," Cryptology ePrint Archive, Jan. 2023.

[12] Kim, Hangi, et al. "PIPO: A lightweight block cipher with efficient higher-order masking software implementations," International Conference on Information Security and Cryptology. Springer, Cham, Vol.

12593, pp. 99-122, Feb. 2021.
〔13〕 Yadav, Tarun, and Manoj Kumar. "Modeling Large S-box in MILP and a (Related-Key) Differential Attack on Full Round PIPO-64/128," International Conference on Security, Privacy, and Applied Cryptography Engineering. Springer, Cham, Vol. 13783, pp. 3-27, Dec. 2022.
〔14〕 Kim, Hyunji, et al. "Deep Learning based Cryptanalysis of Lightweight Block Ciphers, Revisited," Cryptology ePrint Archive, Jul. 2022.
〔15〕 Bao, Zhenzhen, et al. "Enhancing differential-neural cryptanalysis," Advances in Cryptology - ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Springer, Cham, Vol. 13791, pp. 318-347, Jan. 2023.

〈저자소개〉

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

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

서 화 정 (Hwa-Jeong Seo) 종신회원
2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2016년 2월: 부산대학교 컴퓨터공학과 박사 졸업
2015년 4월~5월: 싱가포르 난양공대 인턴쉽
2016년 1월~2017년 3월: 싱가포르 과학기술청 연구원
2017년 4월~2023년 2월: 한성대학교 IT융합공학과 조교수
2023년 3월~현재: 한성대학교 융합보안학과 부교수
〈관심분야〉 암호 구현