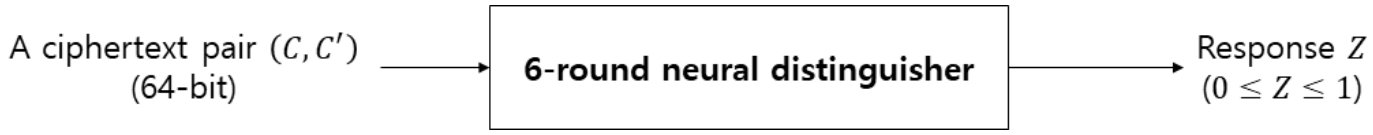
2023 암호분석경진대회

2번 문제

주어진 딥러닝 모델(Neural distinguisher)은 6-라운드로 축소된 SPECK-32/64로 암호화된 암호문을 구별하도록 학습된 모델이다. 제시된 6-round neural distinguisher는 다음 그림과 같이 동작하며 약 75%의 구별 정확도를 보인다.



우리는 위의 neural distinguisher를 기반으로 7-라운드 SPECK-32/64에 대한 키 복구 공격을 수행하려고 한다. 다음 물음에 답하고 키 복구 공격을 수행하시오.

1) Neural distinguisher의 학습 데이터셋은 두 가지의 라벨(0과 1)로 구성되었다. 라벨이 1일 경우에는 암호문 쌍 (C, C')에 대응하는 평문 쌍 (P, P')이 $P \oplus P' = 0x0040/0000$을 만족하며, $P \oplus P' \neq 0x0040/0000$인 암호문 쌍들은 라벨이 0으로 구성된다 (암호화 키는 각 데이터 샘플에 대하여 무작위로 생성된 키가 사용되었다.)
이 데이터셋을 학습한 neural distinguisher의 출력 Z가 의미하는 바를 설명하시오.

2) Neural distinguisher의 출력 Z를 활용하여, 키 복구 공격 시에 추측된 키가 옳은 키인지를 평가할 수 있는 수식을 구성하고 그 원리를 설명하시오.

3) 2)에서 구성한 수식을 기반으로 7-라운드 SPECK-32/64 서브키를 복구하기 위한 알고리즘을 구성 및 설명하고 구현 결과를 제시하시오. (여기서 키 복구 공격 구현을 위한 평문과 키는 임의로 설정하며, 구현 결과가 키를 복구하는 것을 확인할 수 있도록 구성하시오.)

참고: 딥러닝 모델 임포트 및 테스트 코드

```
# Model import
from keras.models import model_from_json
arch = open('arch_neural_distinguisher.json')
json_arch = arch.read()
nr6_speck_distinguisher = model_from_json(json_arch)
nr6_speck_distinguisher.load_weights('weights_nr6_speck.h5')
nr6_speck_distinguisher.compile(optimizer='adam',loss='mse',metrics=['acc'])
# Model test
import speck as sp
x_test, y_test = sp.make_train_data(10**6, 6)
results = nr6_speck_distinguisher.evaluate(x_test, y_test, batch_size=10000)
print('test loss, test_acc: ', results)
```

참고논문: Gohr, Aron. "Improving attacks on round-reduced speck32/64 using deep learning." Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39. Springer International Publishing, 2019.