2024 암호분석경진대회

5번 문제

선형 근사 공격은 평문 P, 암호문 C, 비밀키 K를 이용하여 암호문에 대한 선형근사식 L인 $\alpha \cdot P \oplus \beta \cdot C = \gamma \cdot K$을 구성한다. 이때, α, β, γ는 순서대로 평문 P, 암호문 C, 비밀키 K에 대한 bit location mask이다. 안전한 암호 알고리즘은 선형근사식 L이 성립할 확률 $\Pr_L$이 $1/2$이하이다. 그러나, 만약 암호 알고리즘 내 Substitution이 제대로 동작하지 않을 경우 선형근사식 L이 성립할 확률 $\Pr_L$이 $1/2$을 초과한다. 그리고 공격자는 이와 같은 사실을 이용해 키를 복구할 수 있다.

상기 기술한 선형 근사 공격은 딥러닝을 이용하여 유사하게 구성될 수 있다. 딥러닝 기반 블록암호 키 복구는 고정된 키 K에 대하여 공격자가 n개의 평문과 암호문 쌍을 입력 데이터로 하고, 선형근사식 L의 우변항을 정답 라벨로 학습시켜 모델을 구성한다. 그리고 해당 모델을 이용해 키가 알려지지 않은 평문, 암호문 쌍을 이용해 키를 복구할 수 있다.

이때 아래의 문제에 답하시오.

(1) Feistel 구조 블록 암호 알고리즘에서 선형 공격을 통한 1-bit 키 복구를 위한 알고리즘을 기술하시오.

(2) DES는 Feistel 구조이다. n-라운드로 축소된 DES에서 평문, 암호문, 키의 bit location mask를 선택하고, 선택한 bit location mask를 이용하여 구성한 선형 근사식 L을 기술하시오. 이때 n은 3 이상의 정수 중에 자유롭게 선택할 수 있다.
※ 다음과 같은 Notation을 사용할 수 있음.
P_H 평문 상위 32비트, P_L 평문 하위 32비트, C_H 암호문 상위 32비트, C_L 암호문 하위 32비트,
K_r r라운드의 라운드키, $P[i,j,...,k] = P[i] \oplus P[j] \oplus ... \oplus P[k]$

(3) 딥러닝을 활용하여 문제 (2)에서 기술한 선형근사식 L을 이용한 키 복구 공격 수행 알고리즘을 기술하시오.

(4) 키 복구 공격을 위해 딥러닝 모델의 하이퍼-파라미터와 모델 구조를 상세히 기술하시오.(딥러닝 모델 구성 코드와 학습된 모델 파일 첨부 필수)

(5) 해당 알고리즘을 이용해 학습할 때 사용된 평문-암호문 쌍의 개수와 키 복구 정확도를 작성하시오. (공격 대상 라운드 수, 학습 평문-암호문 쌍의 개수, 키 복구를 위해 사용한 평문-암호문 쌍의 개수, 키 복구 정확도는 상대평가)

(Hint.) Hou, Botao, et al. "Linear attack on round-reduced DES using deep learning." Computer Security-ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14-18, 2020, Proceedings, Part II 25. Springer International Publishing, 2020.