딥러닝 암호분석 논문 리뷰

정보컴퓨터공학과 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

서론

본론

평가

결론

서론

- Deep Learning-Based Cryptanalysis of Lightweight Block Ciphers
- 딥러닝 기반으로 암호 분석
  - 경량 암호: S-DES, Simon, Speck
  - Simon과 Speck의 경우 32/64만 분석
- 분석으로 암호 키 획득
  - Known Plaintext Attack
  - Text-based encryption key

서론

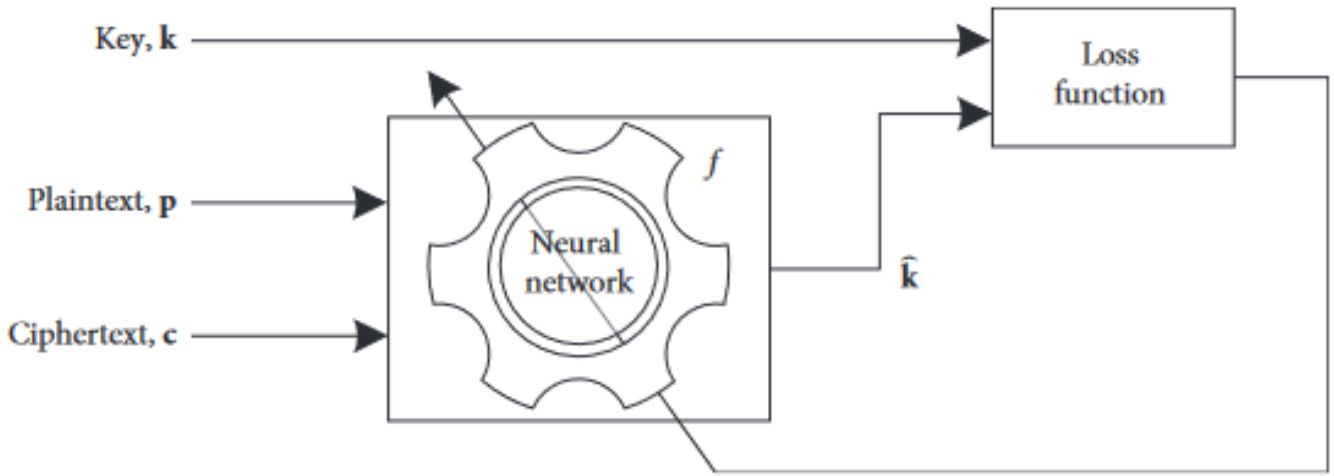
- 알려진 평문 공격(Known Plaintext Attack)
  - 이외에 암호문 단독, 선택 평문, 선택 암호문 공격이 존재
- 공격자가 약간의 평문과 이에 대응되는 암호문을 가진 상황
- 알고 있는 평문/암호문 쌍 외에는 추가적인 정보 없음

본론

- 모든 평문/암호문 쌍은 **다른 키**를 사용하여 암호화
- 정방향 연산
  - 입력 x(평문, 암호문)
  - 파라미터 θ(weight, bias)
  - 활성화함수 ReLU
  - 손실함수 MSE(Mean Square Error)
  - l개의 레이어로 구성

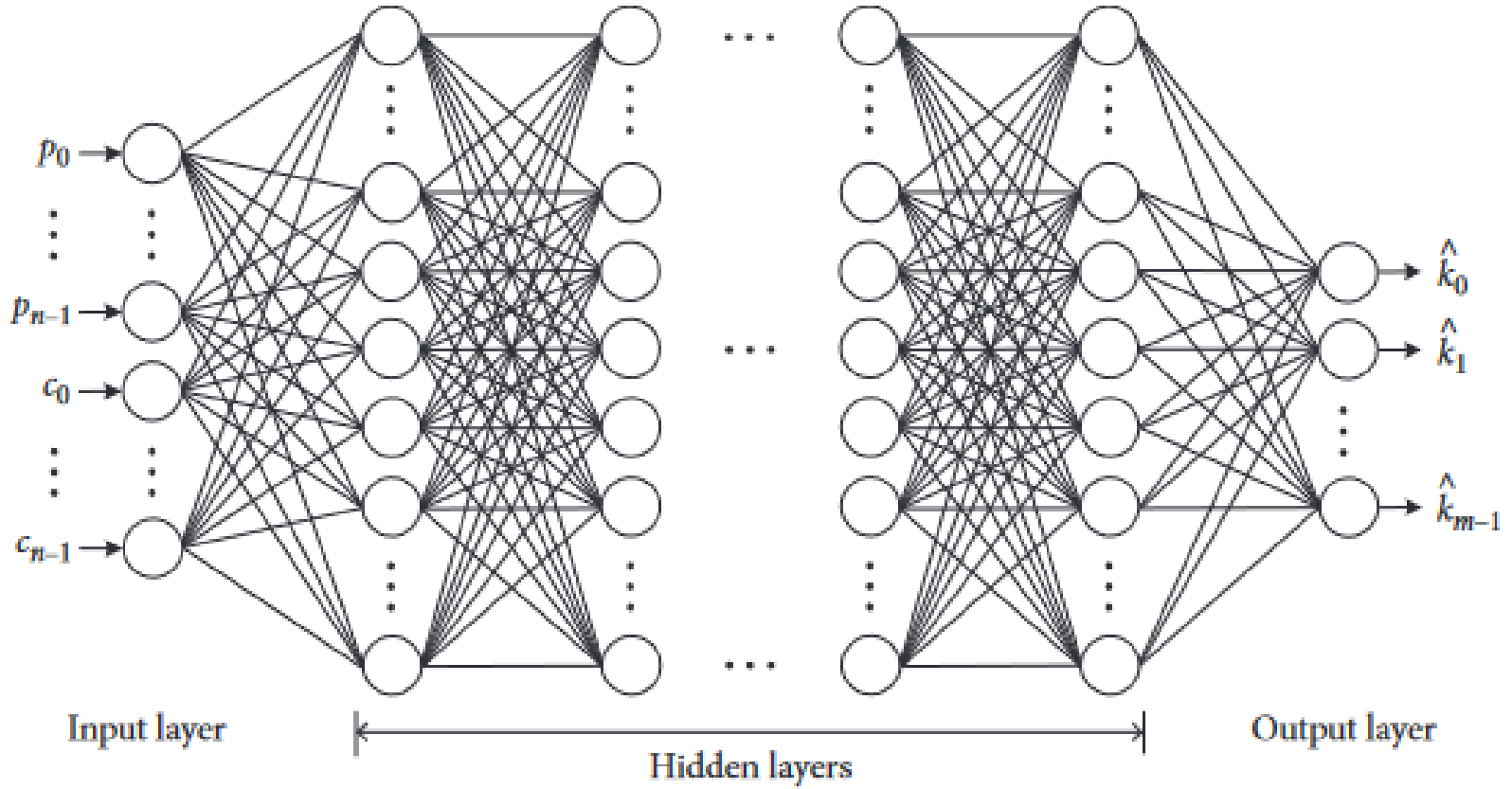
$$f(\mathbf{x};\boldsymbol{\theta}) = f^{(L+1)}\left(f^{(L)}\left(\cdots f^{(1)}(\mathbf{x})\right)\right)$$

$$j^{(l)} = f^{(l)}\left(\sum_i w_{ij}^{(l)} u_i^{(l-1)} + b_j^{(l)}\right)$$



본론

- 입력 평문/암호문 쌍에 따라 예상 키 값 출력



본론

- 데이터 생성 및 학습
- N개의 평문/암호문 쌍 생성
  - 모두 다른 키로 암호화
  - R개는 학습용, S개는 실험용으로 사용
- 손실함수 출력 값 중 **가장 작은 값**으로 파라미터 갱신

$$\theta^* = \arg\min_{\theta} L(f(\mathbf{X};\theta), \mathbf{K})$$

$$\mathrm{MSE} = \frac{1}{N_r \cdot m} \sum_{j=1}^{N_r} \sum_{i=0}^{m-1} \left(\mathbf{k}_i^{(j)} - \widehat{\mathbf{k}}_i^{(j)}\right)^2$$

본론

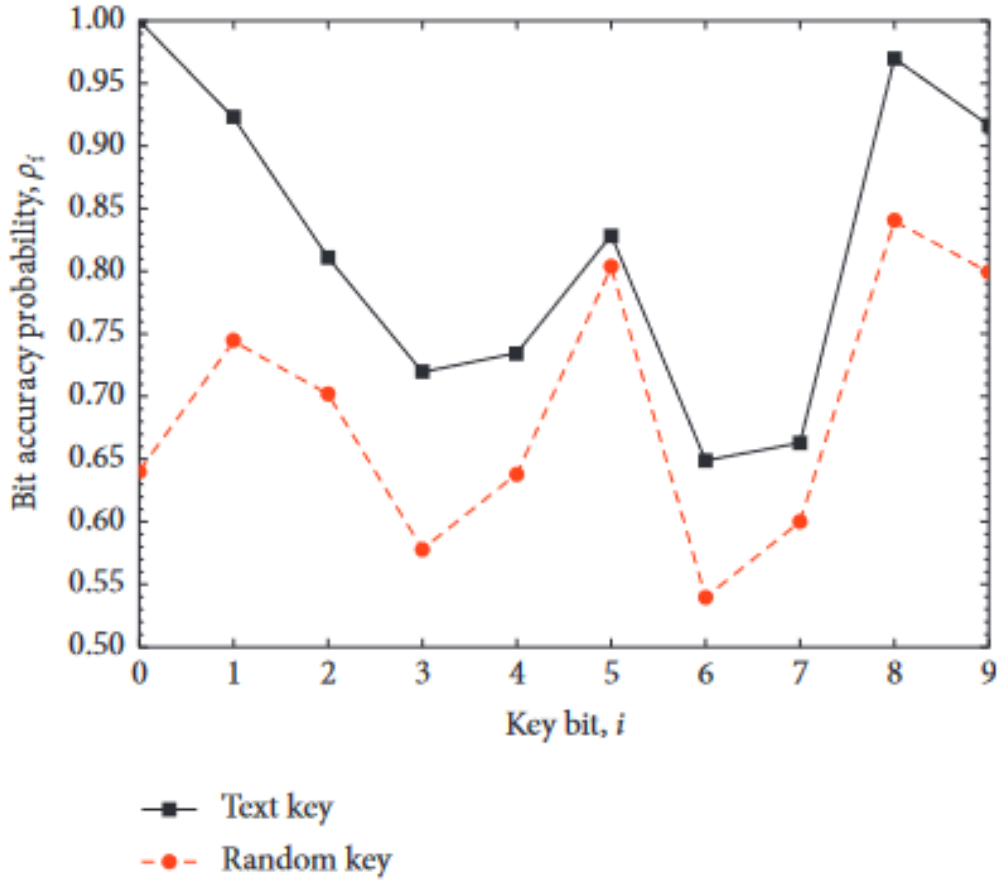
- 실험 단계
- Bit Accuracy Probability (BAP)로 성능 측정
  - 전체 키 대비 맞는 키의 비트 수

$$\tilde{\mathbf{k}}_i = \begin{cases} 0, & \text{if } \hat{\mathbf{k}}_i < 0.5, \\ 1, & \text{otherwise.} \end{cases}$$

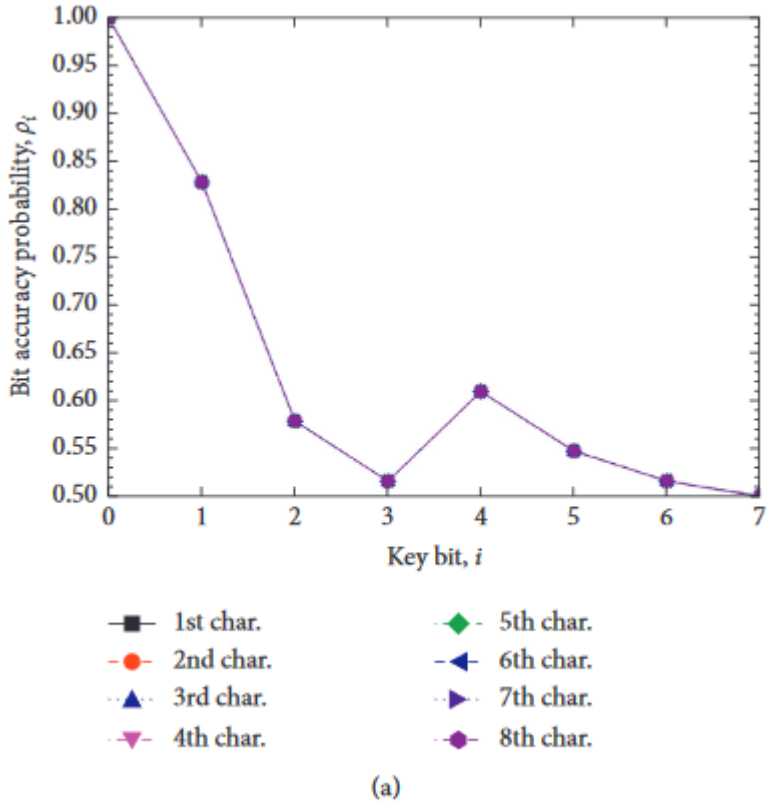
$$\rho_i = \frac{1}{N_s} \sum_{j=1}^{N_s} \mathrm{XNOR}\left(\mathbf{k}_i^{(j)}, \tilde{\mathbf{k}}_i^{(j)}\right)$$

평가

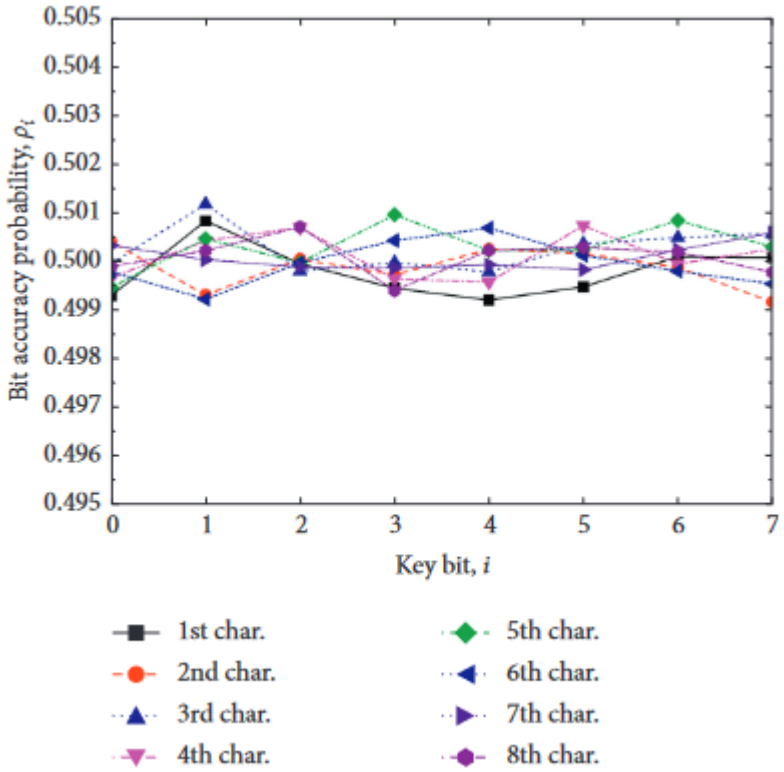
- S-DES
- 60000개의 샘플을 사용
  - 학습 데이터 50000, 실험 데이터 10000
- BAP로 비교 시 최소 0.5389
  - 10비트의 키 중 6번이 제일 안전



평가



(a)



- SIMON과 SPECK의 경우, 전체적으로 S-DES에 비해 낮은 BAP 유지

결론

- S-DES: $2^{8.08}$개의 알려진 평문 존재 시, 90% 확률로 성공
- SPECK: $2^{12.34}$개의 알려진 평문 존재 시,

  99% 확률로 56비트 키 찾기 성공
- SIMON: $2^{12.33}$개의 알려진 평문 존재 시,

  99% 확률로 56비트 키 찾기 성공
- 평문/암호문 **쌍이 매우 많이 필요하다는 한계점** 존재
- 하지만 대량의 **데이터를 확보한다면 키 유출 가능**

Q & A