CPA 사례와 분석

정보컴퓨터공학과 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

CPA 기법

CPA 사례

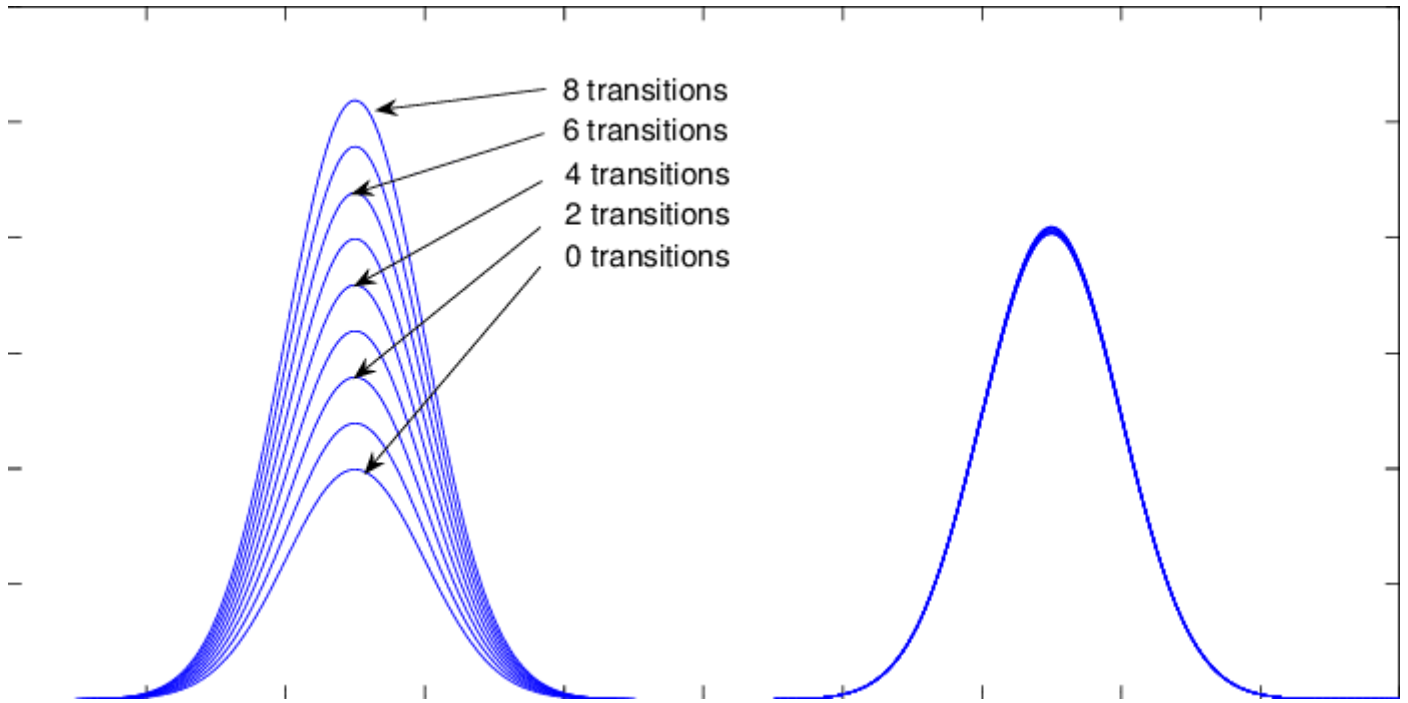
결론 및 향후 과제

CPA 기법

- 부채널 파형 분석 중의 하나
- Correlation Power Analysis
- 추측하고자 하는 값과 실제 값을 비교
  - **Hamming Weight** 모델 사용
  - **피어슨 상관 계수**
  - 가장 높은 상관 계수를 지니는 추측 값이 실제 값

CPA 기법

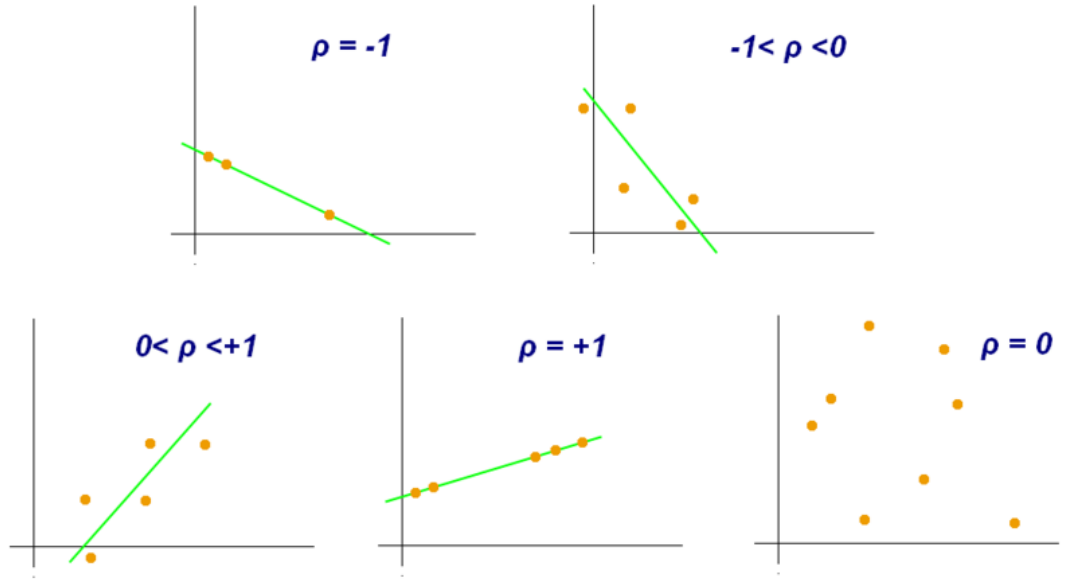
- Hamming Weight 모델
- 기호열에 포함되는 0이 아닌 기호의 수
- 전력 신호 상에서는 0과 1로만 표시되므로, **1의 수**와 동일



CPA 기법

- 상관 관계 분석(Correlation Analysis)
  - 두 변수 간에 **선형적 관계**가 있는지 분석하는 방법
  - 두 변수 간의 연관 정도를 나타내지만 인과 관계는 설명하지 않음
- 피어슨 상관 계수
  - 두 변수 간의 선형 상관 관계를 계량화한 값
  - **일반적인 상관 계수**로 사용 됨

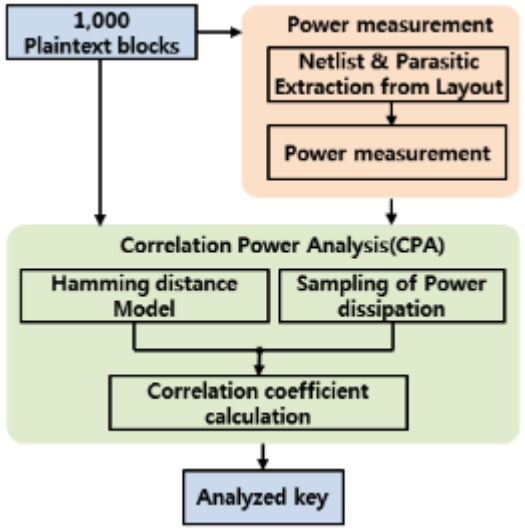
$$r_{XY} = \frac{\sum_i^n \left(X_i - \overline{X}\right)\left(Y_i - \overline{Y}\right)}{\sqrt{\sum_i^n \left(X_i - \overline{X}\right)^2}\sqrt{\sum_i^n \left(Y_i - \overline{Y}\right)^2}}$$

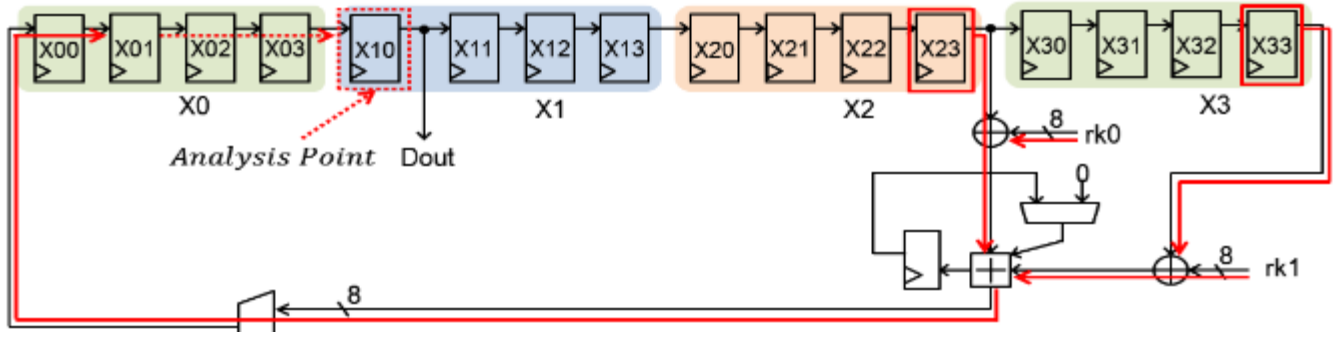


CPA 사례

- LEA에 대한 공격 사례
- 1000개의 파형 수집
- LEA의 블록 중 X1의 상위 8-bit를 공격 지점으로 선정
- 피어슨 상관 계수 식에 따라 상관 계수 r 계산
  - HD: Hamming Distance
  - W: 전력 소모량

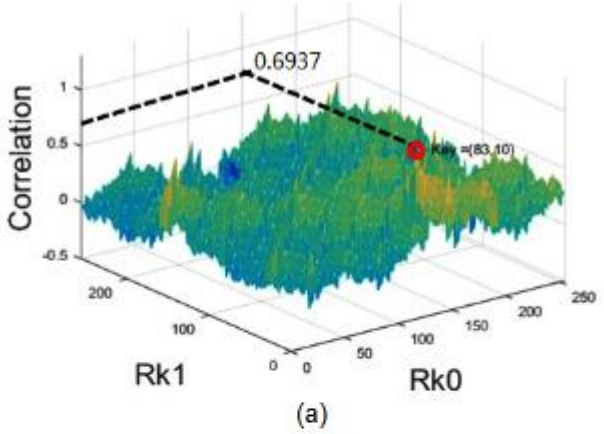
$$r = \frac{\sum (HD - \overline{HD})(W - \overline{W})}{\sqrt{\sum (HD - \overline{HD})^2} \sqrt{\sum (W - \overline{W})^2}}$$



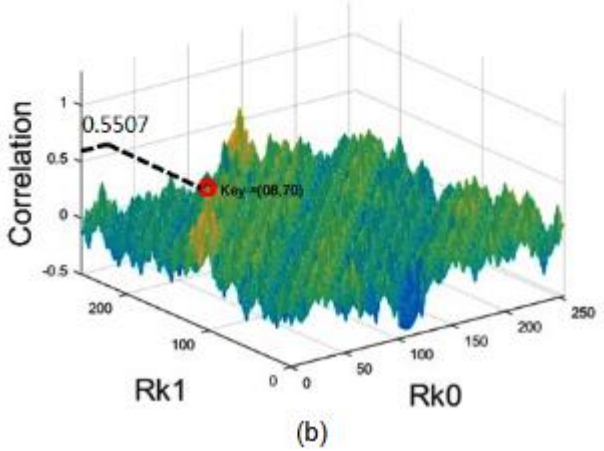


CPA 사례

- 8-bit 단위로 분석
- 32-bit 5, 6번째 블록 값 분석
  - 하위 8-bit 상관 계수: 0.6937
  - 하위 8-bit 키: 0x83, 0x10
  - 상위 8-bit 상관 계수: 0.5507
  - 상위 8-bit 키: 0x08, 0x70
- 획득한 하위 16-bit 키
  - 0x0883, 0x7010
- 이를 반복하여 전체 192-bit 키 획득



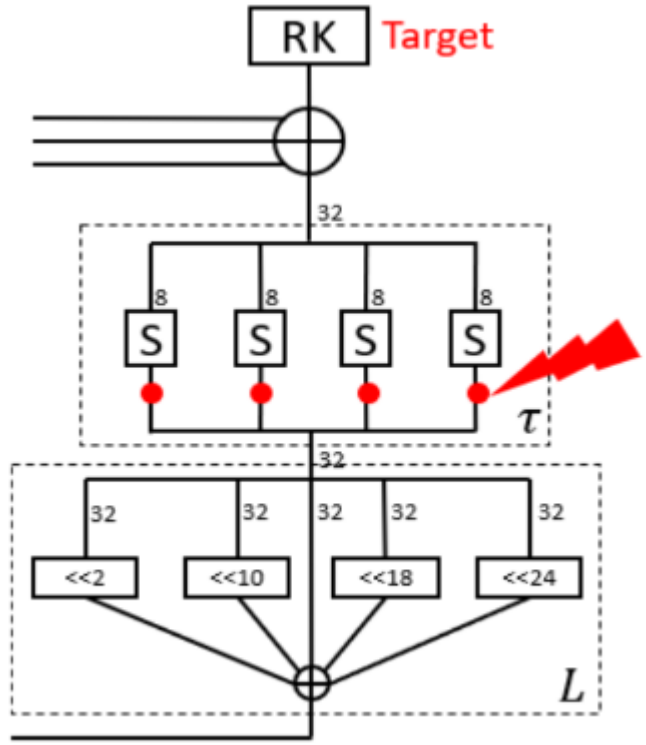
(a)



(b)

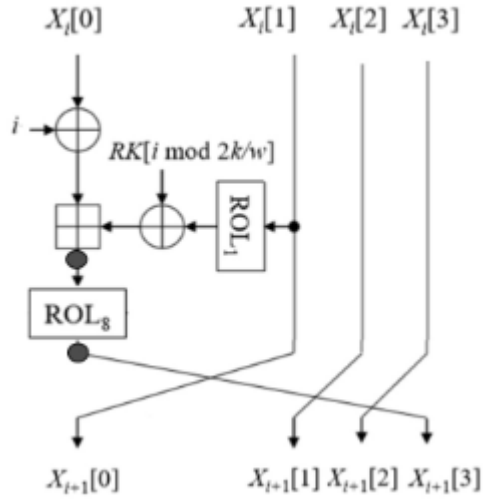
CPA 사례

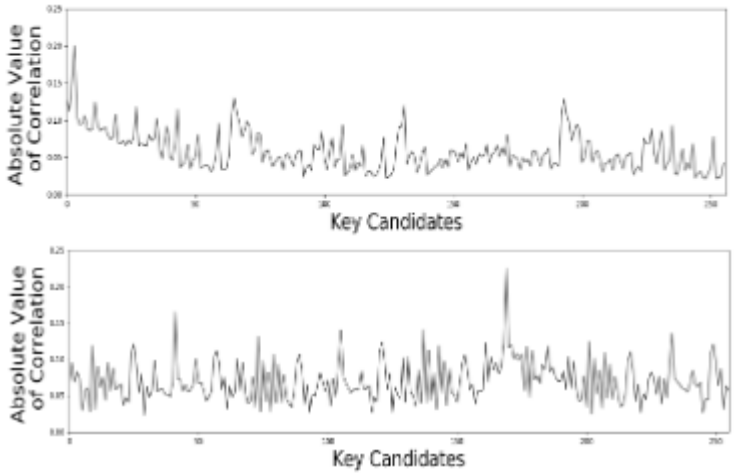
- SM4에 대한 공격 사례
- S-Box 연산 이후 8-bit 값들을 대상으로 공격
  - 하나의 워드 32-bit를 획득하기 위해 4번 반복
  - 상기의 과정을 반복하여 128-bit 비밀키 획득
- 1000개의 파형을 수집
  - 공격 예시로 8-bit 값 중 하나인 0xF1이 가장 높은 상관 계수를 가짐



CPA 사례

- CHAM에 대한 공격 사례
- 5000개 파형 수집
  - 1~8라운드까지 파형만 사용
- 16-bit 라운드 키 블록을 8-bit로 나누어서 공격
  - 상위 8-bit, 하위 8-bit 따로 공격 후 조합
- Rotation 연산 직후를 공격 지점으로 사용
  - 하위 값: 0xA9, 상위 값: 0x03





결론 및 향후 과제

- CPA 공격에서 가장 중요한 것은 공격 지점 선정
  - 비선형 연산 지점에서 **선형 관계를 파악**
- 대부분의 공격은 **8-bit 단위**로 이루어짐
  - 8-bit 단위로 0x00~0xFF의 상관 계수 파악
  - 진보된 형태의 brute force
- **NIST Lightweight를 분석**하여 CPA를 시도
  - ChipWhisperer를 사용
  - 8-bit를 사용하는 경우에는 추후 경량 마스킹 구현도 시도 가능

Q & A