부채널 공격

정보컴퓨터공학과 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

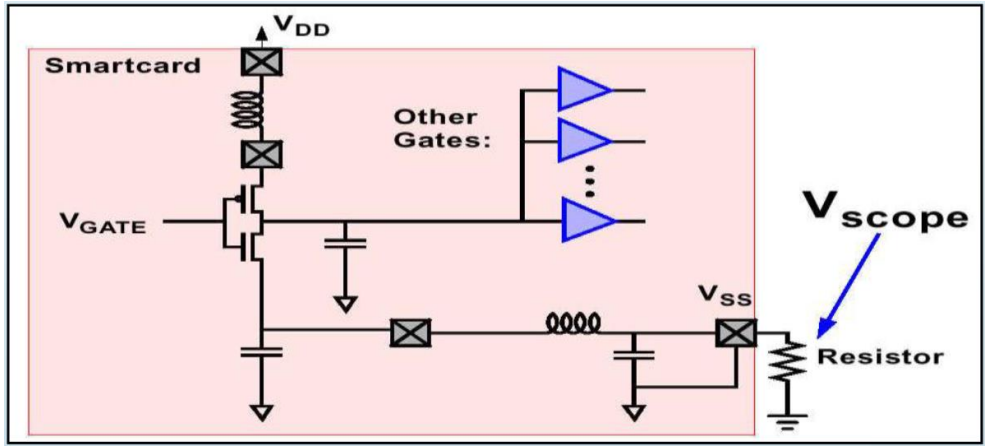
부채널 분석

- 정의
  - 암호기능 동작 시 **부가적인 정보**를 수집/분석하여 비밀정보를 획득하는 기법
  - 연산시간, **소비전력**, 소리, 전자기파
  - 비침투 공격, 수동적 공격 등으로 분류

- 종류
  - Timing attack: 수행시간을 활용
  - Power Analysis Attack: 소비전력신호 이용
    - SPA, DPA, CPA

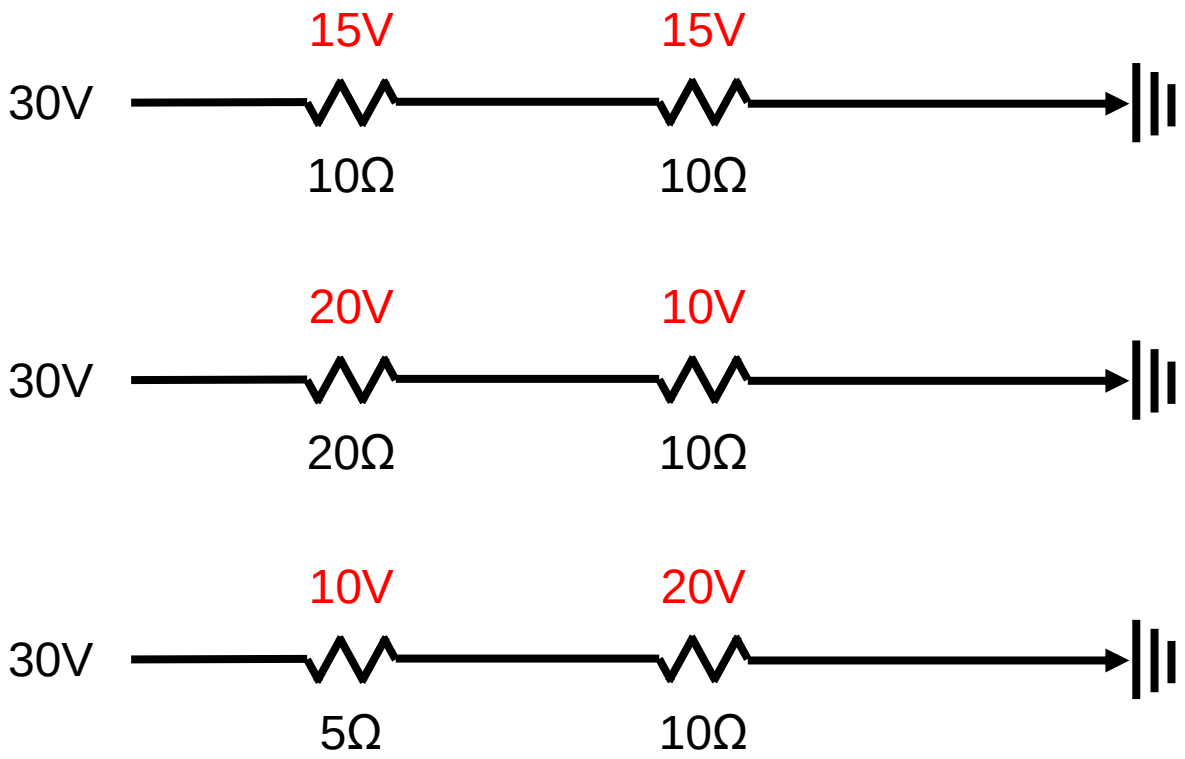
전력 분석 공격

- 1998년 P. Kocher에 의해 처음으로 제안
- 하드웨어 암호모듈의 **접지** 또는 **전원부**에 저항을 연결하여 전력 측정
- 공격 방법에 따라 분류
  - Simple Power Analysis
  - Differential Power Analysis
  - Correlation Power Analysis
- **소비 전력에 대한 기준 필요**



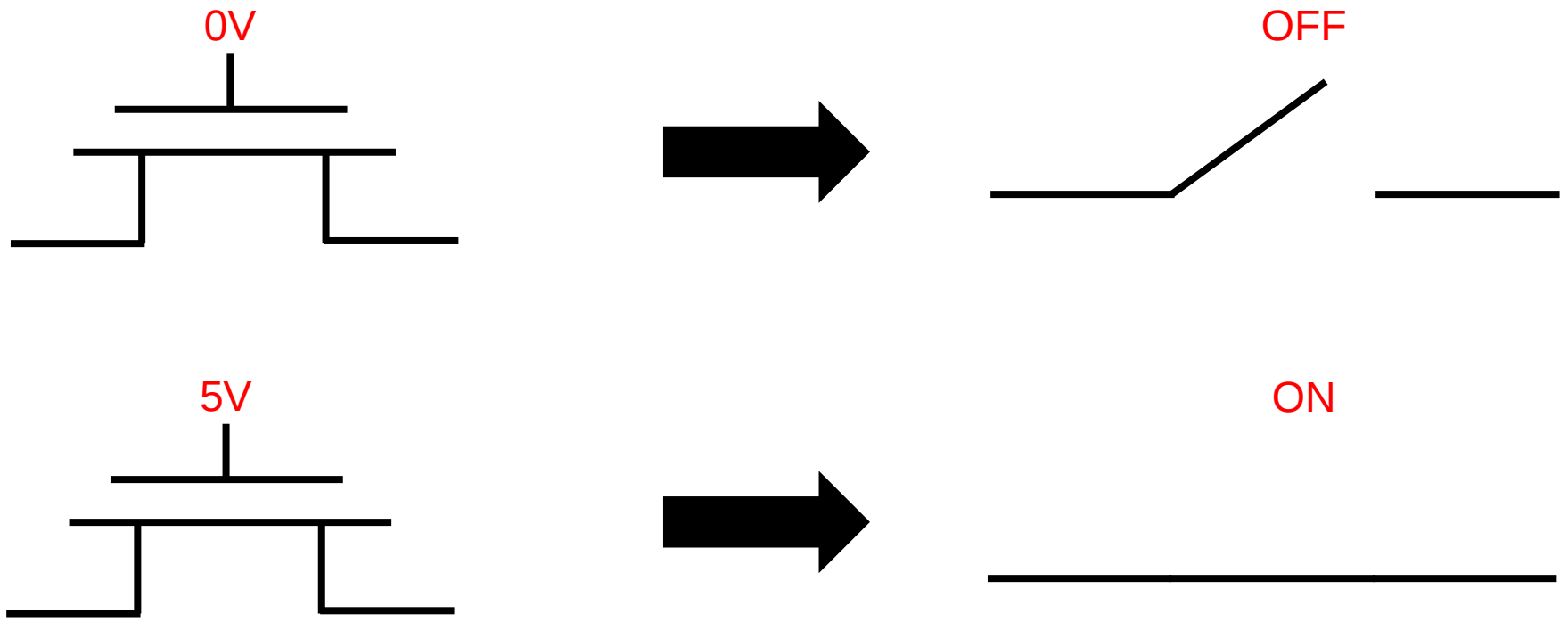
전력 분석 공격

- 소비 전력 측정 개념



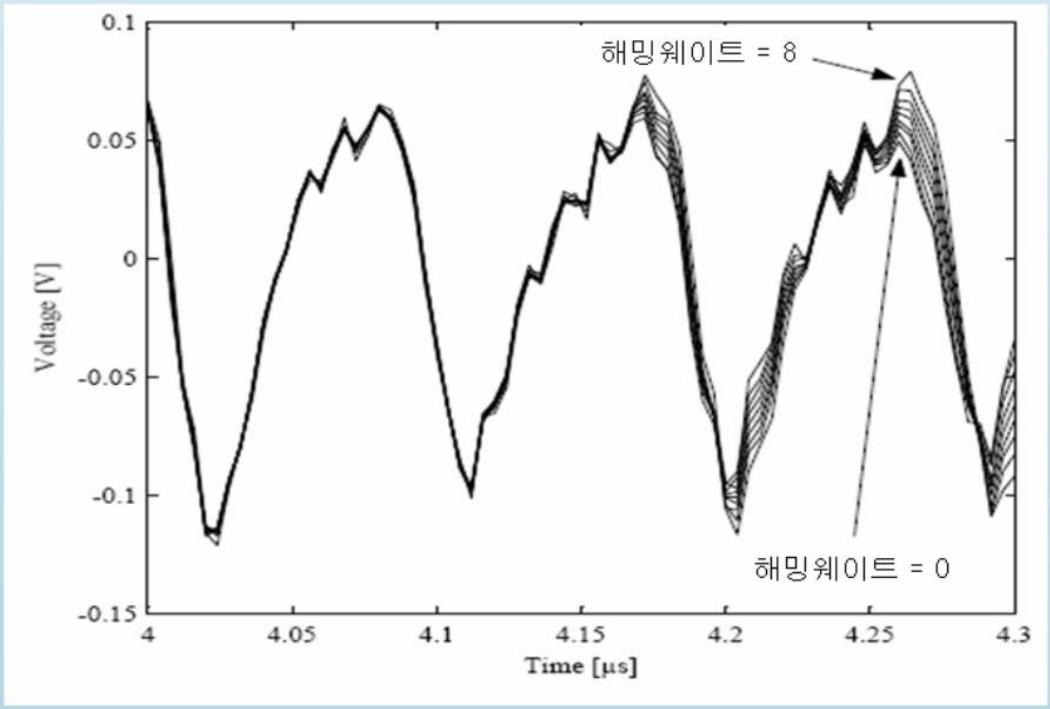
전력 분석 공격

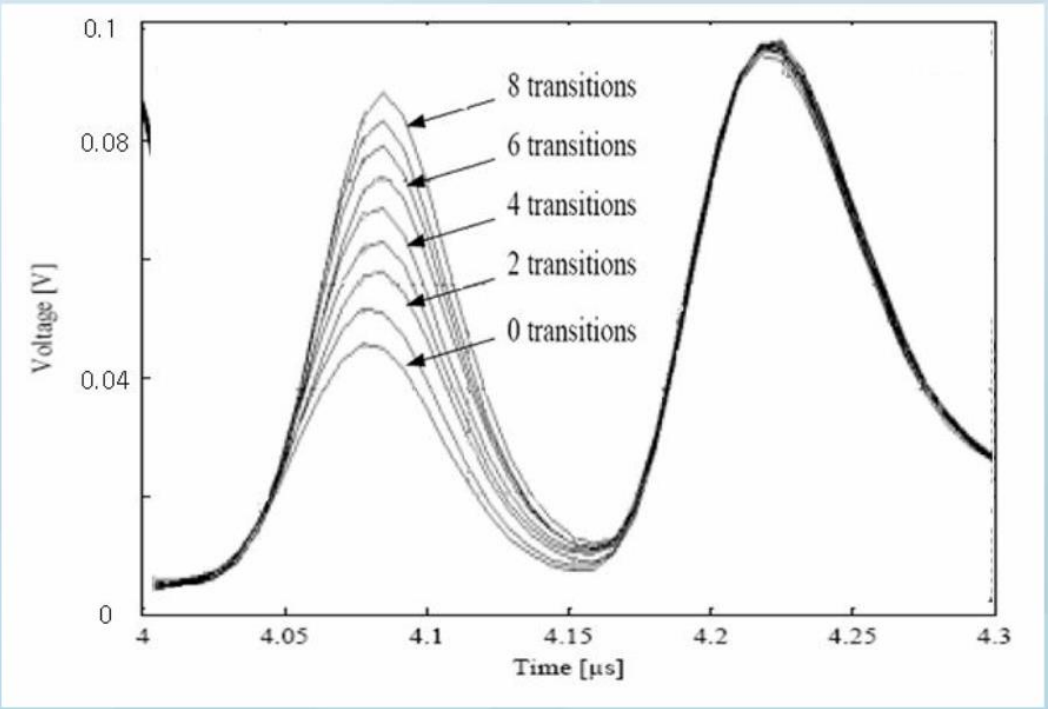
- CMOS 동작 개념
  - **부채널 분석에서는 CMOS 동작 개념을 사용**



전력 분석 공격

- 소비 전력 모델
  - Hamming weight model: 1값이 0값보다 전력 소비가 큼
  - Hamming distance model: 데이터의 상태 변화 시 전력 소비가 큼





전력 분석 공격: SPA

- **하나 혹은 적은 수의 전력 파형**을 수집/분석
- 활용
  - 키 추출
  - DPA 공격 위치 파악
  - 알고리즘 구조 파악

- SPA 공격으로는 키 추출은 쉽지 않다
- **하지만 DPA 공격 등을 위한 준비 과정으로 사용 가능**

전력 분석 공격: DPA

- 다수의 파형을 **통계적으로 분석**하여 비밀키 추출
- SPA와의 차이
  - 다수의 전력 파형 필요
  - 파형 수집과 비밀키 추출 단계가 구분
  - 연산 데이터의 소비전력 모델 정보 활용
  - 통계적 기법 사용
- 활용
  - 블록암호 키 추출

전력 분석 공격: DPA

- 공격자가 **키를 예측**하여 분류한 **두 그룹 간의 차이 여부**를 판단
- DPA 시행 전 가정
  - 부채널 신호는 연산 데이터에 의존할 것
    - Hamming weight, Hamming distance model
  - 암호 알고리즘의 동작 방식은 공개되어 있을 것
  - 공격자는 충분한 수의 부채널 신호를 수집할 수 있을 것
  - 공격자는 암호 알고리즘의 입력 또는 출력을 알 수 있을 것

전력 분석 공격: DPA

- DPA 수행 절차
  - 1. 임의 평문을 사용하여 소비전력을 측정
  - 2. 추측한 키와 입력 평문을 이용하여 중간 값의 Hamming weight를 계산
  - 3. 계산 결과에 따라 전력 신호를 분류
  - 4. 양분한 데이터를 각각 평균을 계산하여 차분신호 계산
    - S0 = {Si[j] | D(key, data) = 0 or Low Hamming weight}
    - S1 = {Si[j] | D(key, data) = 1 or High Hamming weight}
  - 5. 차분신호가 0보다 크면 올바른 키, 0과 같으면 틀린 키

전력 분석 공격: CPA

- DPA의 파생
- 키를 예측하여 계산한 **중간 값**과 **부채널 신호와의 연관성**
- CPA 수행 순서
  - 다수의 임의 평문을 입력하여 소비전력을 측정
  - 추측한 키와 입력 평문을 이용하여 중간 값의 Hamming weight를 계산
  - 측정한 소비 전력과 계산결과 간의 상관관계 계산
    - $\mathrm{Corr}(x_1, \ldots, x_s, y_1, \ldots, y_{1s}) = \frac{\sum_{s=1}^{S}(x_s-\bar{x})(y_x-\bar{y})}{\sqrt{\sum_{s=1}^{S}(x_s-\bar{x})^2}\sqrt{\sum_{S=1}^{S}(y_s-\bar{y})^2}}$
  - 상관도가 가장 높게 나오는 추측키가 올바른 키

CPA 시연

- 제공된 파이썬 스크립트를 참고하여 CPA 구현
  - CPA를 통한 AES 1라운드 비밀키 분석
  - 16바이트 비밀키 추출
- 제공 파형 1,000개의 비밀키 추출

Q & A