

전력 분석 공격

<https://youtu.be/Xpctzf0p6vl>

전력 분석 공격 ?

- 전력분석 공격(Power Analysis Attack)

- ✓ 암호 기기의 전력 소비 패턴을 분석하여 비밀 정보를 알아내는 부채널분석 공격 기법

- ✓ 종류

- 단순 전력분석 (Simple Power Analysis Attack, SPA)

- 차분 전력분석(Differential Power Attack, DPA)

전력 분석 공격 ?

- 단순 전력분석 공격

- ✓ 공격자가 암호 연산을 한 번 또는 수차례 구동시키면서 수집한 전력 소비량의 시간에 따른 변화 양상을 주로 시각적으로 해석하는 방식으로 공격 진행

- ✓ ex) RSA 공개키 암호시스템

- 모듈러 지수승 연산을 위해 사용되는 모듈러 제곱 연산과 모듈러 곱셈 연산 :전력 소비 패턴 매우 다름
 - 해당 패턴을 분석하면, 두 연산을 쉽게 구별 가능
 - RSA의 복호화 연산에 사용되는 비밀 지수 값을 SPA를 통해 상당히 정확하게 복구 가능

전력 분석 공격 ?

- 차분 전력분석 공격

- ✓ SPA보다 더 강력한 공격 방법
- ✓ 암호 연산을 여러 차례 구동시킨 후 얻을 수 있는 전력 소비량 정보를 다양한 신호 처리 방법을 사용하여 분석하여 암호 기기 내부에 저장된 비밀 정보를 얻어냄.
- ✓ 전력 소모 파형 분석하는 것뿐만 아니라, 전력 소모량과 비밀키의 상관관계 통계적으로 분석
- ✓ 분석을 위해 암호장치가 임의의 평문 P 와 비밀키 K 를 이용하여 암호화 연산 수행
 - 전력소모 파형을 수집하여 표본화
 - 추측한 비밀키를 이용하여 연산 수행
 - 분류 함수에 따라 전력 소모 파형을 분류하여 평균의 차분 신호를 구함

전력 분석 공격 ?

- 상관관계 전력 분석 (Correlation Power Analysis, CPA)
 - ✓ 평문을 선택하면 대응하는 암호문을 얻을 수 있는 상황에서의 공격
 - ✓ 공격자가 한꺼번에 선택한 평문들에 대한 암호문이 주어진다는 가정 하에 복호화 키를 찾는 공격
 - ✓ 차분 전력 분석 공격과 달리, 비밀키를 추정하여 얻은 암호화 연산 중간값을 해밍무게(Hamming Weight)모델 또는 해밍거리(Hamming Distance) 모델로 변환
 - ✓ 해밍무게 모델
 - SW로 구현된 암호장치에 적용되는 전력 소모 모델
 - '1'의 값을 갖는 비트 수와 소비 전력이 동일한 패턴을 갖는 모델을 의미
 - 해밍무게 : 비트 내에서 0이 아닌 성분 비트의 개수
 - $c = (0010111)$ 에서 0이 아닌 성분 = 4 , 해밍무게 = 4
 - ✓ 해밍거리 모델
 - HW로 구현된 암호장치에 적용되는 전력 소모 모델
 - 스위칭된 비트의 개수와 소비 전력이 동일한 패턴을 갖는 모델을 의미
 - 해밍거리 : 두 비트에서 비트 값이 서로 다른 비트 자리 위치의 개수
 - ex) 010 과 000의 해밍 거리 : 1

01001010 | 해밍무게 = 3

00000000 | 해밍무게 = 0

해밍거리 : 3

전력 분석 공격 ?

- 두 비트열 $R0, R1$ 에 대해,
해밍거리 모델 : $HD(R0, R1)$ 해밍무게 모델 : HW

$$\begin{aligned} & \mathbf{HD(R0, R1)} \\ &= \mathbf{HW(R0 \oplus R1)} \end{aligned}$$

전력 분석 공격 방법

- 일반적인 전력 분석 공격 단계

- ✓ 데이터 수집 단계

- 랜덤 (or 공격자에 의해 임의로) 선택된 평문 (or 암호문)을 이용하여 암호화(or 복호화) 연산을 수행
 - 해당 연산에 대한 소비전력 파형 수집

- ✓ 데이터 분석 단계

- 비밀키(의 일부분)에 대해 그 값을 예측
 - 예측한 후 예측값과 입력된 평문(or 암호문)을 이용하여 내부 연산값 계산
 - 계산값의 유효성을 수집된 전력소비 파형을 이용하여 검증
 - 이 과정을 반복
 - 최종적으로 비밀키 전체값을 복구

전력 분석 공격 가능한 이유

- 스마트 카드 IC와 같은 저전력 기기의 경우,
 - ✓ 자체 전원을 사용 X, 외부에서 전력을 공급 ↑
 - 외부 전력 공급량을 모니터링하게 되면, 실제 암호 기기가 소비하는 전력량을 매우 정확히 측정 가능
 - ✓ 전력 소비량을 줄이기 위해, 암호 연산 도중 암호 연산과 관계없는 주변 기기의 동작을 정지 ↑
 - 암호 연산만이 소비하는 전력량을 매우 정확하게 측정가능
 - **전력분석 공격 수월하여 적용 가능**
- PC의 경우, 암호 연산 도중에 백그라운드에서 다양한 응용 프로그램이 동작하는 경우가 많음
 - 응용프로그램의 동작 : 암호 연산만의 전력 소비량 측정에 장애물로 적용
 - 전력 분석 공격은 고사양기기에 잘 사용X
 - 전자기장분석 공격의 경우, 암호 연산기의 정확한 위치 식별 가능 → PC등의 고사양 기기에도 적용

전력 분석 공격 가능한 이유

- 전자 기기 내부에 저장된 값에 따라 저장과 처리에 필요한 전력 소비 패턴 다름
 - ✓ 전력 분석 공격은 이런 패턴의 차이 이용
 - ✓ 내부 비트값의 변화가 없는 경우와 계속 변화하는 경우, 전력 소비량 비교를 통해 구분 가능
 - 전력 분석 공격이 가능한 이유

전력 분석 공격 가능한 이유

- 공격 진행되는 방식과 관련

- 데이터 분석 단계에서 입력된 평문 (or 암호문)과 기기에 저장된 비밀키의 예측값을 이용하여 내부 연산값 계산

- 성공적인 공격 수행을 위해, 평문(or 암호문)의 정확한 값을 공격자가 알고있다는 가정 필요

- ✓ 평문(or 암호문)의 정확한 값을 공격자가 알고있다는 가정이 성립하지 않은 경우,

- 공격자가 평문(or 암호문)에 대한 정보를 알지 못하면, 전력분석 난이도 \uparrow or 공격 불가

전력 분석 공격 가능한 이유

- 마스크 기법

- ✓ 평문(or 암호문)의 정확한 값을 공격자가 알고있다는 가정 성립 → 공격 방어
- ✓ 블록 암호 알고리즘에 대한 대표적인 DPA 대응 기법 중 하나
- ✓ 메시지에 대한 암호화 복호화 연산을 수행하기 전에 난수를 이용
- ✓ 평문을 마스크하고 마스크된 데이터에 대해 암호화 복호화 연산 수행
- ✓ 외부에서 관찰가능한 소비 전력 패턴과 연산 중간값의 관련성을 축소 or 제거 할 수 있다는 사실 기반

마스킹 기법


유한체 K_1, K_2

함수 $f: K_1 \rightarrow K_2$,

입력 마스크 차수 d_{in} , 출력 마스크 차수 d_{out}

XOR연산: K_1, K_2 의 덧셈 연산

함수 f 에 (d_{in}, d_{out}) - 차 (불)마스킹 기법 적용 과정

임의의 $x \in K_1$ 에 대해서, 

- 1) $x_1, x_2, \dots, x_{d_{in}} \in K_1$ 을 랜덤하게 선택한다.
- 2) $x_0 = x \oplus x_1 \oplus x_2 \oplus \dots \oplus x_{d_{in}}$ 을 계산한다.
($(x_0, x_1, \dots, x_{d_{in}})$ 는 x 의 d_{in} -차 마스크 또는 함수 $z = f(x)$ 의 d_{in} -차 입력 마스크라고 한다)
- 3) $(x_0, x_1, \dots, x_{d_{in}})$ 을 사용하여
 $z_0 \oplus z_1 \oplus \dots \oplus z_{d_{out}} = f(x)$ 를 만족시키는
 $z_0, z_1, \dots, z_{d_{out}} \in K_2$ 를 계산한다.
($(z_0, z_1, \dots, z_{d_{out}})$ 은 $z = f(x)$ 의 d_{out} -차 마스크 또는 함수 $z = f(x)$ 의 d_{out} -차 출력 마스크라고 한다)
- 4) 마스킹 기법이 안전하다는 것은 $z_0, z_1, \dots, z_{d_{out}}$ 의 계산 과정에서 원래의 입력값인 x 에 대한 (어떠한) 정보의 노출도 없어야 함을 의미한다.

Q & A

