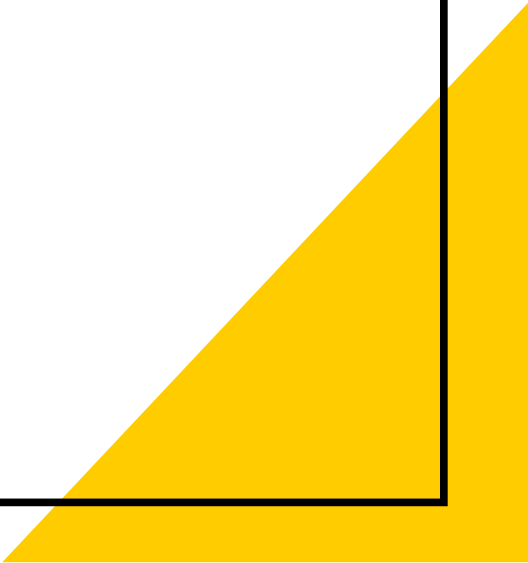


# Side Channel Attack ( Power Analysis )

IT정보공학과 신명수

# 목차

1. About Side Channel Attack
  2. SPA (Simple Power Analysis)
  3. DPA (Differential Power Analysis)
  4. CPA (Correlation Power Analysis)
- 
- A large yellow triangle is positioned in the bottom right corner of the slide, pointing towards the top right.

# 1. About Side Channel Attack

- 부채널 정보
  - 암호 장비에서 암호 알고리즘이 실행될 때 평문-암호문 쌍 이외의 암호 동작 소요시간, 소비 전력량, 방출되는 전자기파 등을 말함.
- 부채널 분석
  - 부채널 정보를 통해 비밀키와 같은 정보를 취득하는 분석 방법

# 1. About Side Channel Attack

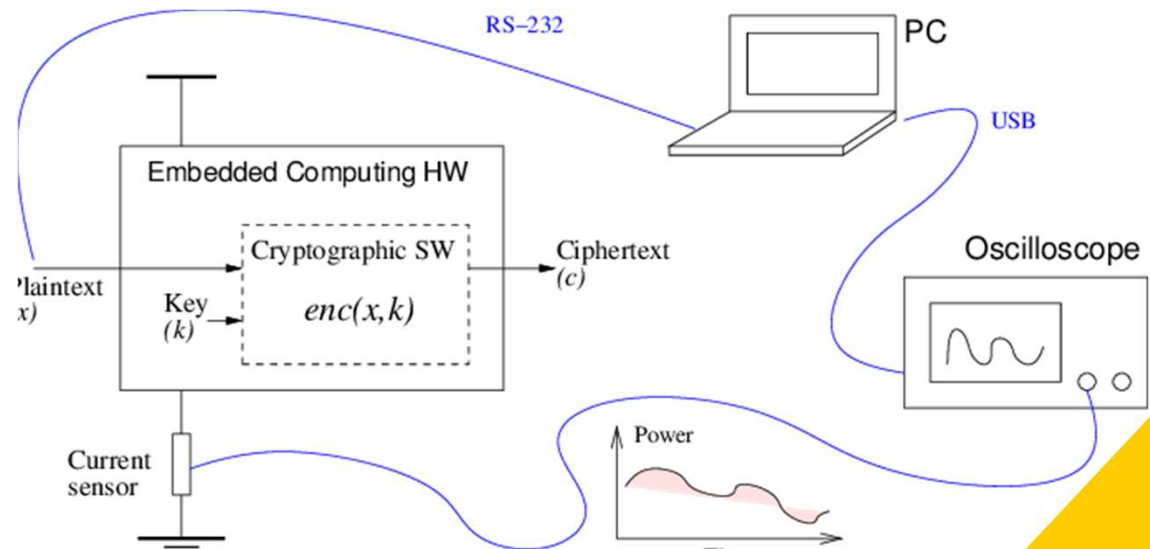
## Timing Analysis

- 연산이 수행될 때의 시간 차이를 이용하는 공격 기법.
- 암호 시스템은 서로 다른 입력 데이터를 처리하기 위해 조금씩 다른 시간이 소비된다.  
Ex. 분기 및 조건문, 캐시 hit 횟수, 곱셈 및 나눗셈 연산 등
- 암호 연산의 실행 시간이 비밀키와 연관된 정보에 의존한다는 가정을 기반함.

# 1. About Side Channel Attack

## Power Analysis

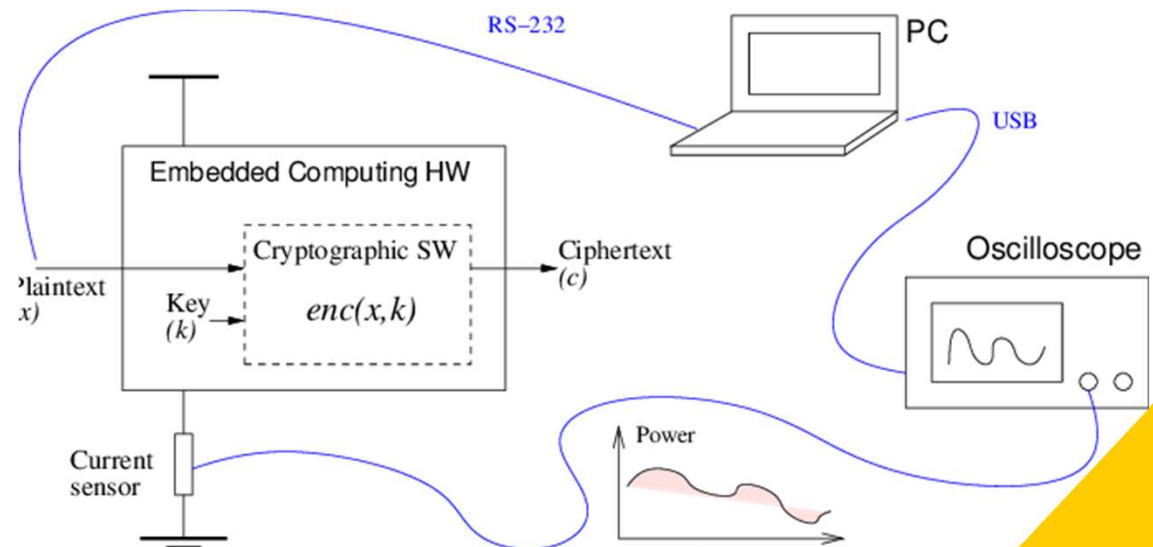
- 암호 모듈이 처리하는 데이터와 연산에 따라서 순간 소비 전력의 차이를 사용하는 공격 기법.
- 암호 모듈이 설치된 기기에 저항과 오실로스코프를 연결해 파형을 수집.



# 1. About Side Channel Attack

## Power Analysis

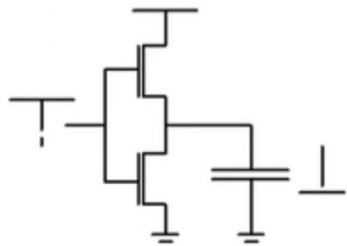
- 소비 전력은 암호 모듈이 동작할 때 입력받은 정보에 따라서 약간의 차이를 보이게 된다.
- 전력 분석 공격은 데이터와 소비전력의 연관성을 바탕으로 공격



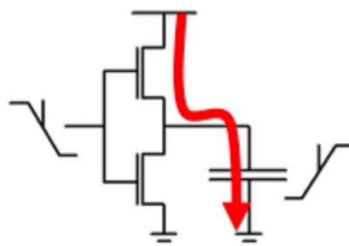
# 1. About Side Channel Attack – Power Analysis

## 내부 연산 데이터와 소비 전력 사이 연관성

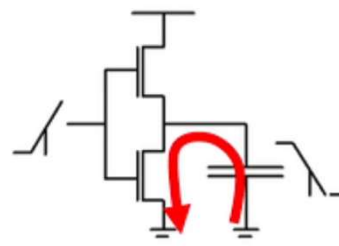
회로에서 사용하는 CMOS 인버터 (NOT gate)



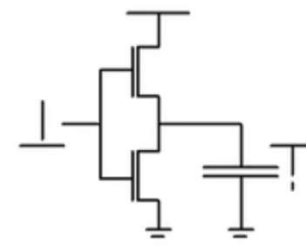
0-0 transition



0-1 transition



1-0 transition



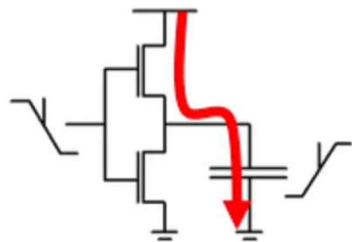
1-1 transition

# 1. About Side Channel Attack – Power Analysis

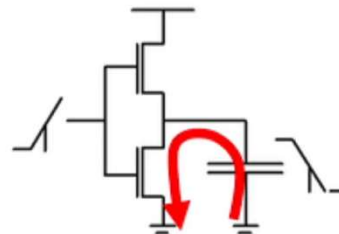
## 내부 연산 데이터와 소비 전력 사이 연관성

데이터가 0에서 1로 바뀔 때, 1에서 0으로 바뀔 때 전력 소비가 발생한다.

- 전력 분석은 데이터가 바뀔 때 소비 전력의 차이를 바탕으로 공격을 한다.



0-1 transition



1-0 transition



# 1. About Side Channel Attack – Power Analysis

## 데이터 상태 변화 모델링

- Hamming Weight Model (the number of bits set to 1)

$$HW(x) = \sum x[i], \quad x = (x[0], \dots, x[n-1]) \in \{0, 1\}^n$$

$$ex. HW(110100101) = 5.$$

- Hamming Distance Model

$$HD(x_0, x_1) = HW(x_0 \oplus x_1)$$

$$ex. HD(0010, 0001) = 2.$$

# 1. About Side Channel Attack – Power Analysis

## 데이터 상태 변화 모델링

- 데이터가 변경될 때 전력 소비량이 발생  
-> 비트가 바뀌는 만큼 전력 소비가 일어나는 것을 모델링함.

# 1. About Side Channel Attack – Power Analysis

## 수집하는 소비 전력

1. 연산 의존 소비 전력
2. 데이터 의존 소비 전력
3. 노이즈
4. 상수 요소 (디바이스가 동작하는데 필요한 소비 전력 등)

# 1. About Side Channel Attack – Power Analysis

전력 분석 공격은 데이터와 전력 소비 간의 관계를 통해 공격

-> 노이즈의 요소가 영향을 미칠 수 있음.

## 2. SPA (Simple Power Analysis)

- 하나 혹은 적은 수의 전력 파형을 분석하여, 민감 정보를 추출하는 전력분석기법을 말한다.
- 소비전력량, 연산시간 차이를 이용해 키 추출 가능.
- 분석 및 공격 위치 검색에 사용됨.

## 2. SPA (Simple Power Analysis)

- 공개키 암호의 비밀키 추출에 효과적이다.
- 소수의 전력 파형만으로 가능
- 비밀키를 실시간으로 추출 가능
- 명령어 수행 여부 활용
- 통계적 기법 미적용 -> 신호 노이즈에 취약하다.

## 2. SPA (Simple Power Analysis)

### SPA로 공개키 암호 비밀키 추출

ex. RSA 모듈러 지수승 연산 구현 부분을 공격하여 키를 추출

*Algorithm1. Modular exponentiation ( $X^d \bmod N$ )  
calculation using left to right binary method.*

*input:  $X, N, d = (d_{k-1}, d_{k-2}, \dots, d_0)$*

*output:  $Z = X^d \bmod N$*

*$Z \leftarrow 1$*

*For  $i = k - 1$  down to 0 do*

*$Z \leftarrow Z \times Z \bmod N;$*

*if( $d_i = 1$ )then*

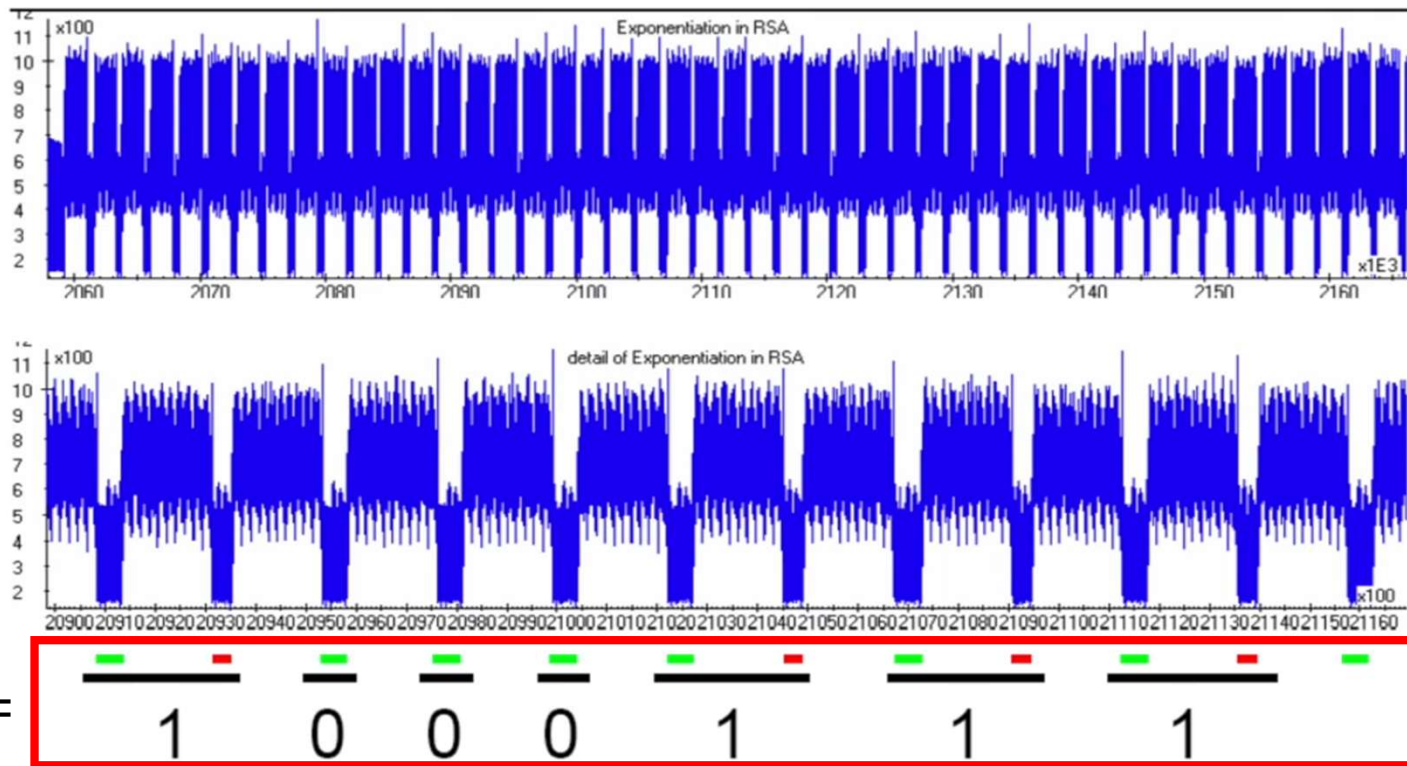
*$Z \leftarrow Z \times X \bmod N;$*

*end*

*end*

*return  $Z$ ;*

## 2. SPA (Simple Power Analysis)

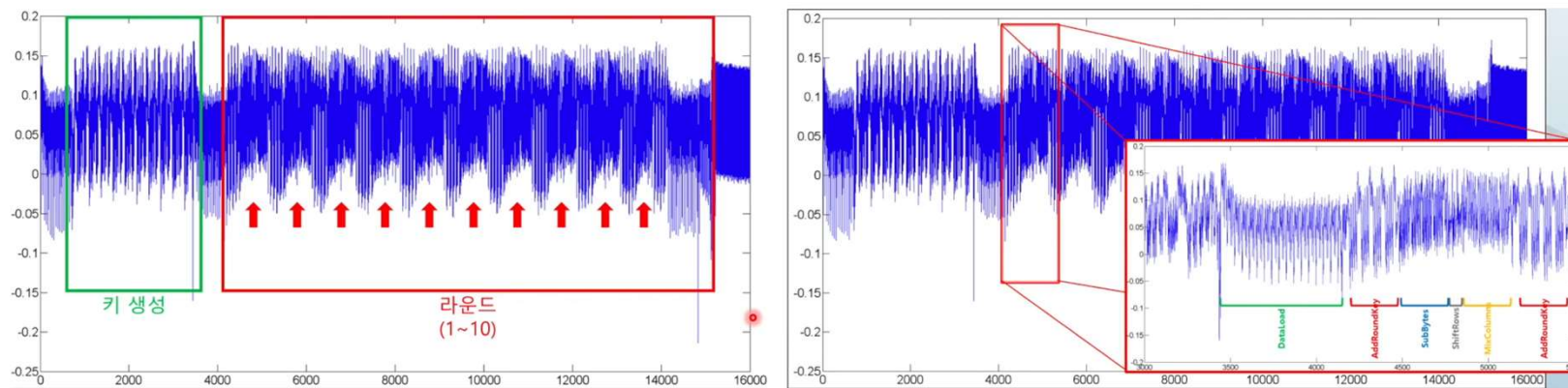




## 2. SPA (Simple Power Analysis)

### 암호 알고리즘 구조 파악

DPA나 CPA를 위해 공격 위치를 파악하기 위해 사용하거나 리버싱에 사용될 수 있다.



AES-128 10 round Encryption

### 3. DPA (Differential Power Analysis)

- 다수의 파형을 통계적으로 분석하여 암호 알고리즘 비밀키를 추출하는 방법.
- 블록암호 비밀키 추출에 효과적임.

### 3. DPA (Differential Power Analysis)

- 다수의 전력 파형을 사용함.
- 파형 수집과 비밀키 추출 단계를 구분한다.
- 연산 데이터의 소비 전력 모델 정보를 활용한다.
- 통계적 기법을 활용해 신호 노이즈에 내성이 있다.

### 3. DPA (Differential Power Analysis)

#### DPA 공격 조건

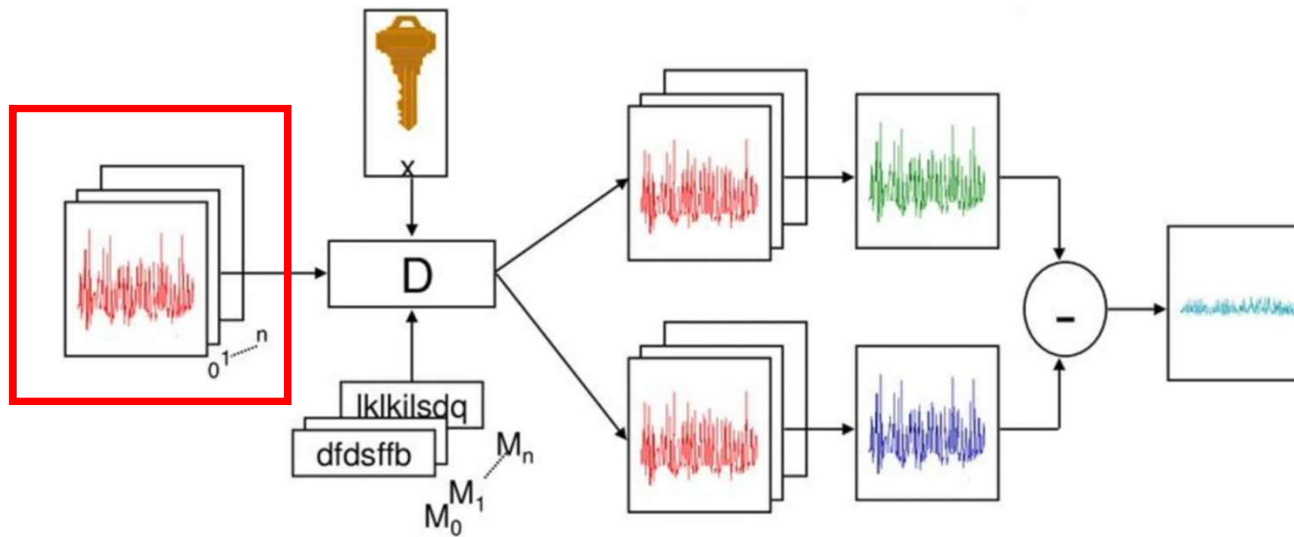
1. 부채널 신호는 연산 데이터에 의존한다.
2. 암호 알고리즘의 동작 방식은 공개되어있다.
3. 공격자는 충분한 수의 부채널 신호를 수집할 수 있다.
4. 공격자는 암호 알고리즘의 입력 또는 출력을 알 수 있다.

### 3. DPA (Differential Power Analysis)

#### 블록암호에 대한 DPA 공격 과정

1. 다수의 임의의 평문을 입력하여 소비전력을 측정

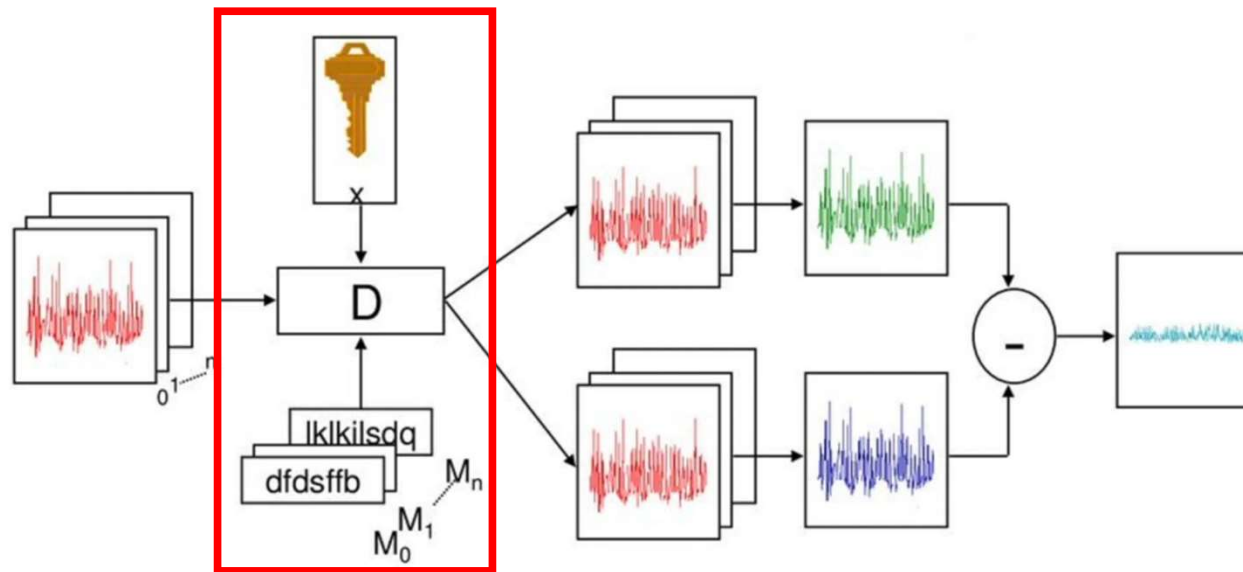
Input 데이터 – Trace(파형)의 한쌍 ex. AB – (2, 5, 7, 3, 8, 9, 3), 05(5, 7, 3, 0, 9, 8, 6) .....



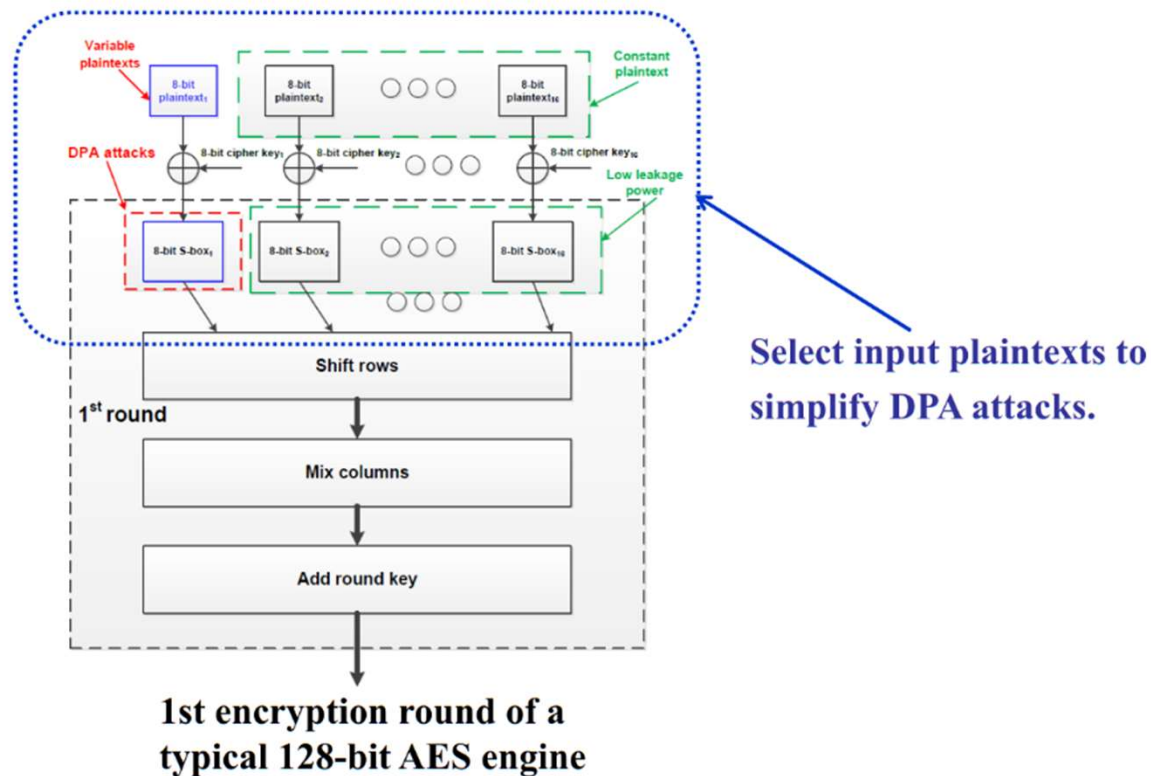
### 3. DPA (Differential Power Analysis)

#### 블록암호에 대한 DPA 공격 과정

2. 추측 키(1 byte)와 평문을 이용하여 중간값 연산 ex.  $Sbox(p \oplus key)$



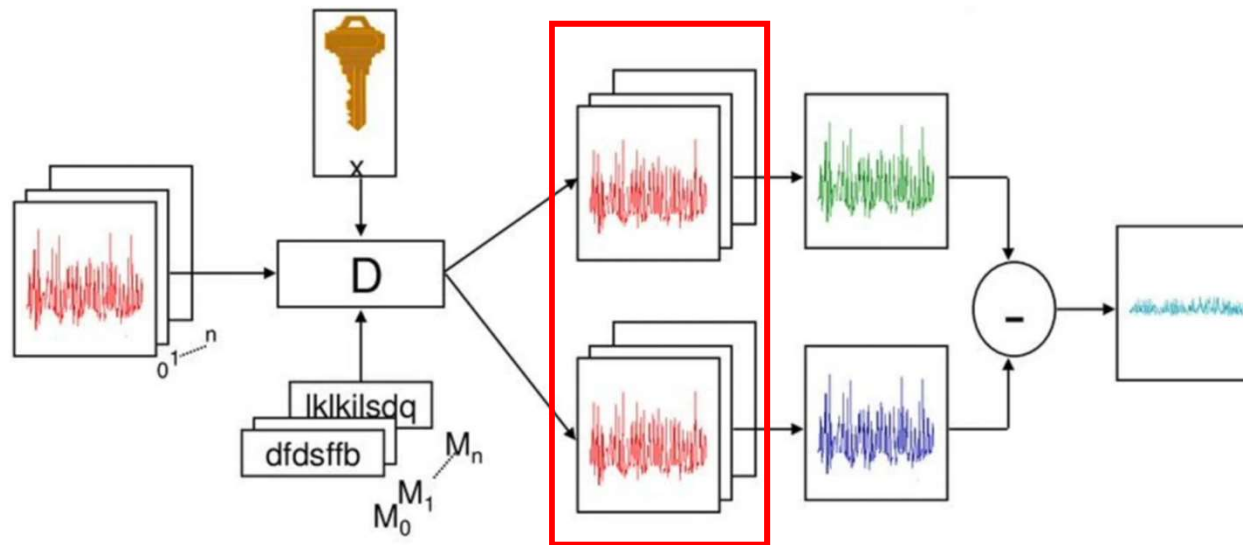
### 3. DPA (Differential Power Analysis)



### 3. DPA (Differential Power Analysis)

#### 블록암호에 대한 DPA 공격 과정

3. 중간값의 hamming weight를 계산하여 값에 따라 분류





### 3. DPA (Differential Power Analysis)

#### 블록암호에 대한 DPA 공격 과정 예시

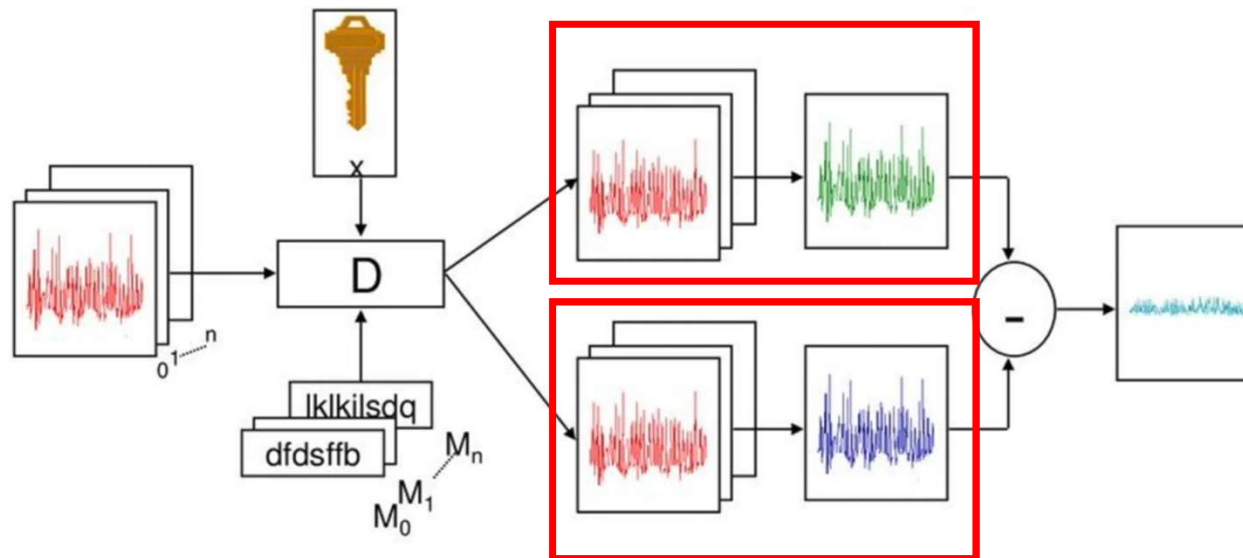
2. 추측 키(1 byte)와 평문을 이용하여 중간값 연산 ex.  $Sbox(p \oplus key)$   
현재 계산하고 있는 추측 키가  $0xC2$  이고,  $Sbox(0xAB \oplus 0xC2) = 0x54$  라 하자.

3. 중간값의 hamming weight를 계산하여 값에 따라 분류  
 $0x54(01010100)$  이므로  $HW(0x54) = 3$  이다.  
 $HW(Sbox()) = 4$  를 기준으로 Small group 과 Big group 로 분류

### 3. DPA (Differential Power Analysis)

#### 블록암호에 대한 DPA 공격 과정

4. 양분한 데이터 그룹 각각 평균 소비전력을 구한다.

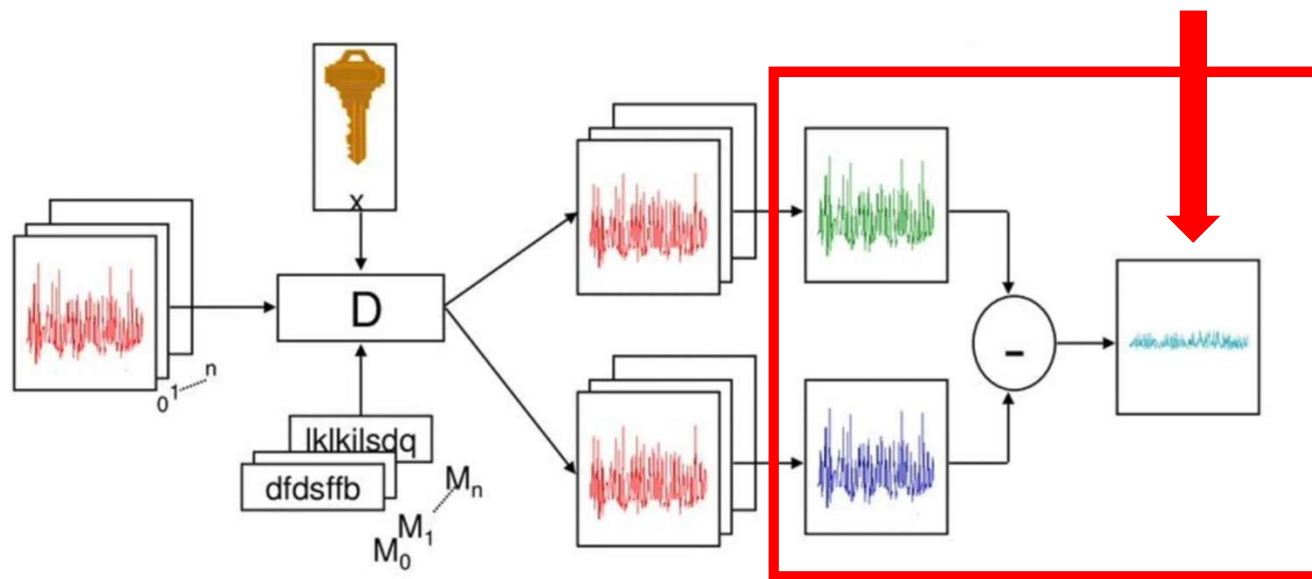


### 3. DPA (Differential Power Analysis)

#### 블록암호에 대한 DPA 공격 과정

##### 5. 차분 신호를 계산

추측 키 0xC2에 대한 차분 신호



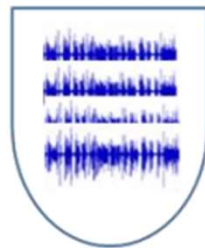
# 3. DPA (Differential Power Analysis)

여러개의 추측키에 대해 차분파형을 생성하여 비교

HW는 bit 1의 수  
예) 11001100 = HW(4)

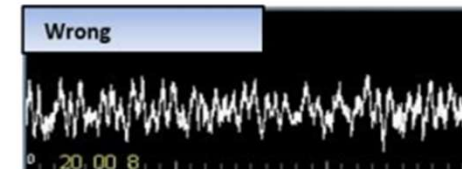
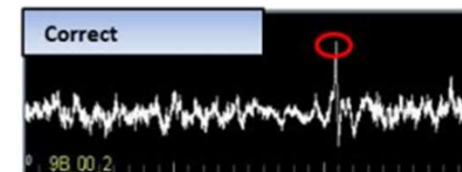
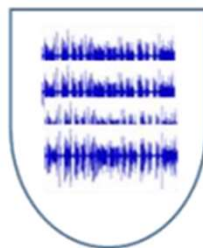
KEY GUESS

HW 0,1,2,3,4



—

HW 5,6,7,8



### 3. DPA (Differential Power Analysis)

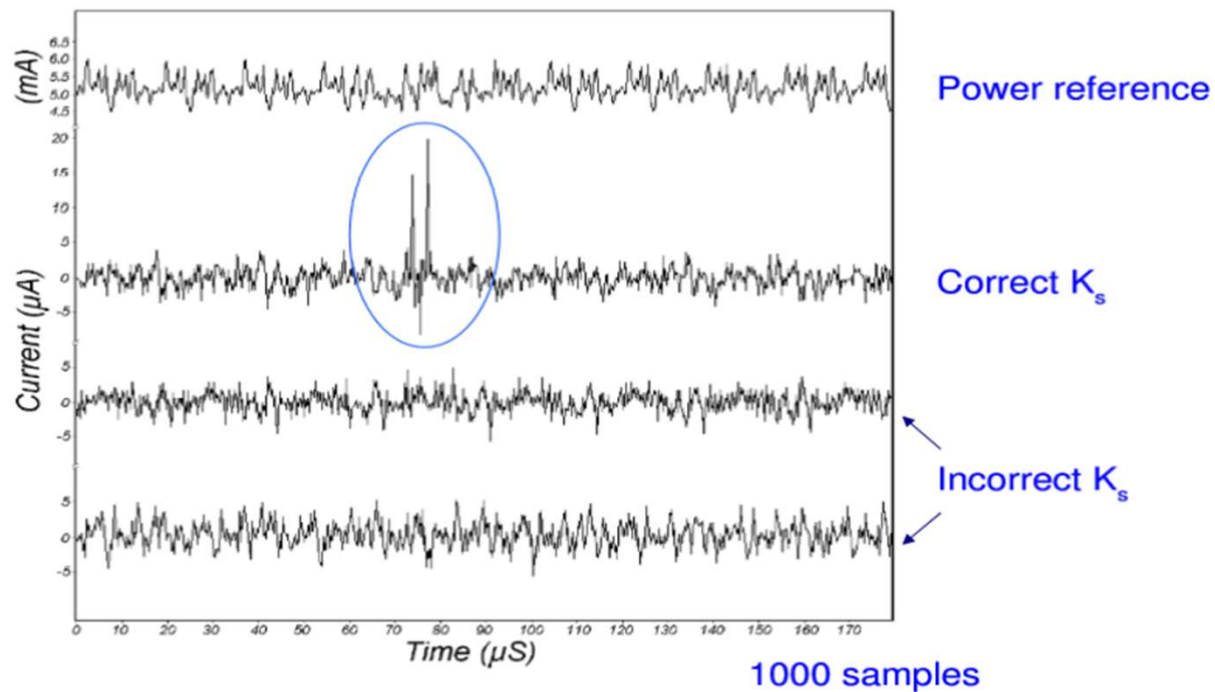


Figure 8. DPA traces, one correct and two incorrect, with power reference [7].

## 4. CPA (Correlation Power Analysis)

- 다수의 파형과 Hamming Weight 간의 상관 관계를 계산하여 비밀 키를 추출하는 방법.
- Hamming Weight 집단과 소비 전력 집단 간 가지는 선형적 관계를 기반으로 공격.

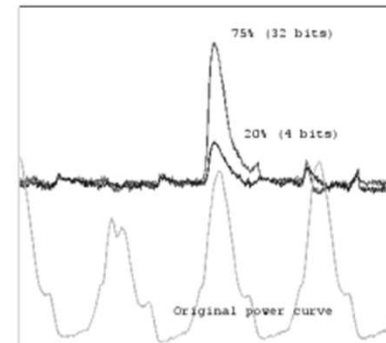
## 4. CPA (Correlation Power Analysis)

- 다수의 임의 평문을 입력하여 소비 전력 측정
- 추측한 키와 평문을 이용하여 중간값을 Hamming Weight 계산
- 측정한 소비 전력과 Hamming Weight 간의 상관 관계 계산
- 상관도가 가장 높게 나오는 추측키 = 올바른 키

## 4. CPA (Correlation Power Analysis)

CPA 에서 사용되는 상관 계수

$$\rho(X, Y) = \frac{E(XY) - E(X)E(Y)}{\sqrt{E(X^2) - E(X)^2} \cdot \sqrt{E(Y^2) - E(Y)^2}}$$



**Fig. 2.** Two correlation peaks for full word (32 bits) and partial (4 bits) predictions. According to theory the 20% peak should rather be around 26%.