# MASKING COUPLING EFFECT 최신 동향

권혁동* 권용빈* 서화정 *†
- 한성대학교 대학원 IT융합공학부

## 요 약

● 부채널 공격을 방어하기 위해 마스킹 기법이 개발되었으나 마스크 값이 소실되는 커플링 현상이 발견

● 커플링 현상에 대해 조사하며 이를 완화할 수 있는 방법에 대해 고찰

## 부채널 공격

● 암호 장비의 암호 알고리즘 등을 공격하는 것이 아닌 빛, 소리 등의 부가요소를 공격하는 기법

● 단순 분석: 통계적 수단 없이 전력 소모 패턴을 파악

● 차분 분석: 통계적 수단, 소모 모델과 실제 측정 값과 비교

● 전력 소모 등의 특성을 감추는 것으로 부채널 공격 방어 가능

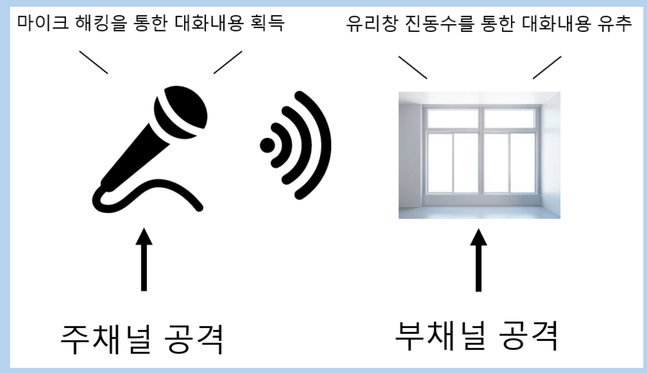


Fig 1. 부채널 공격 비유

## 마스킹 기법

● 원본 값에 마스크 값을 씌워 전력 분석을 방해하는 기법

● 연산자에 따라 부울, 산술 마스킹 기법으로 분류

● 마스크 값은 고정 또는 난수 값 사용

● 커플링과 글리치 현상에 무력화

$$x' = x \oplus r$$

$$x' = (x - r) \bmod 2^k$$

Fig 2. 상) 부울 마스킹 / 하) 산술 마스킹

## 커플링 현상

● 마스크 값이 소실되는 현상으로 커플링 발생시 부채널 공격에 무방비 상태가 됨

● Overwrite: 동일한 저장 공간에 데이터를 덮어 쓸 경우

● Memory Remnant: 메모리 상의 값을 불러올 때 이전 값의 잔여 데이터로 인하여 발생

● Neighbour Leakage: 인접한 저장 공간에 데이터를 저장 할 경우

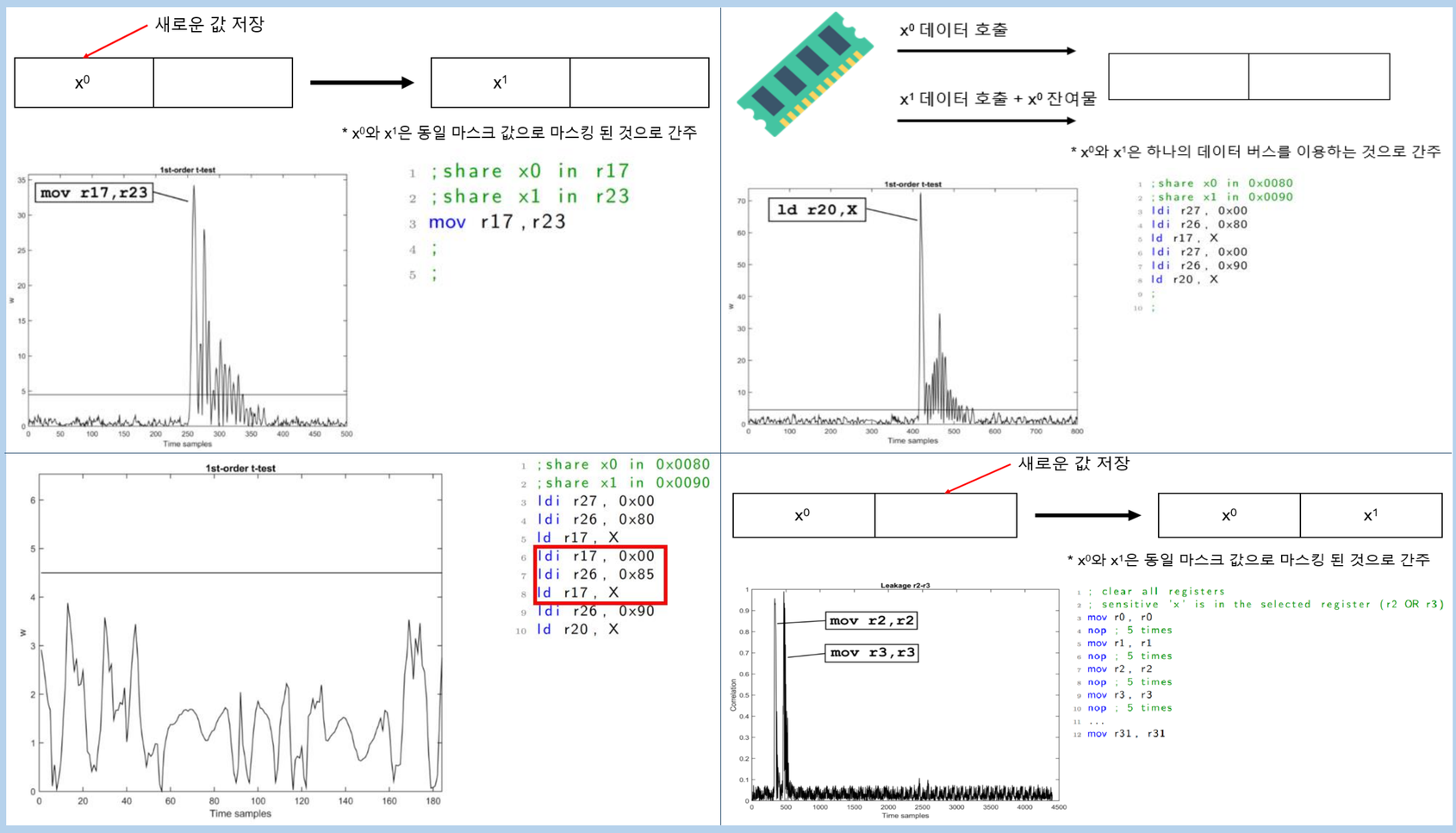


Fig 3.
좌상) Overwrite 효과
우상) Memory Remnant 효과
좌하) Memory Remnant 완화 현상
우하) Neighbour Leakage 효과

## 결 론

● 부채널 공격은 암호 알고리즘을 공격하지 않고 장비의 부채널 정보를 파악하여 공격하는 기법

● 마스킹 기법은 부채널 분석을 어렵게 만들어서 공격을 방어하는데 유효함

● 커플링 현상으로 인하여 마스크가 소실되면 부채널 공격에 다시 취약해짐

● 커플링 현상을 방지하는 기법을 찾아낼 수 있도록 지속적인 연구가 진행중