

# 온라인 세미나

---

2019. 02. 17.

한성대학교 IT응용시스템공학과  
권혁동

<https://youtu.be/U9crHm57wYE>

# 연구 진행 방법

---



- 국민대학교 연구실과 연계 연구
- 코드 분석 및 취약점 가능성 부분을 검토 후 공유

# 타깃 디바이스

---



- Atmel AVR
- 8비트 프로세서
- 구조가 단순함
- 연산능력은 떨어짐

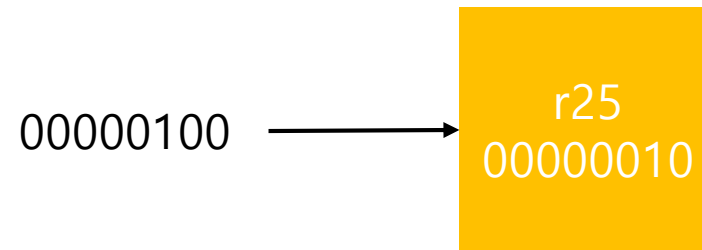
# 마스킹

---

- 원본 데이터에 임의의 마스크 값을 추가
- 파형 분석 시 마스크 값으로 인해 원활한 관측이 어려움
- 본 연구에서는 마스킹이 임의로 소실되는 현상을 연구  
= 커플링 현상

# 커플링 현상

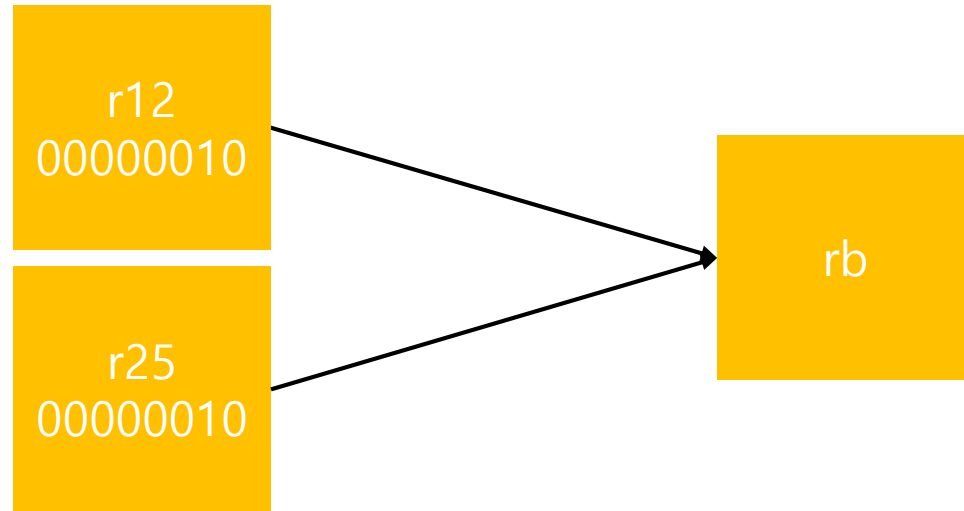
---



- Overwriting Effect
- 값이 있는 레지스터에 새로운 값을 덮어 쓸 경우

# 커플링 현상

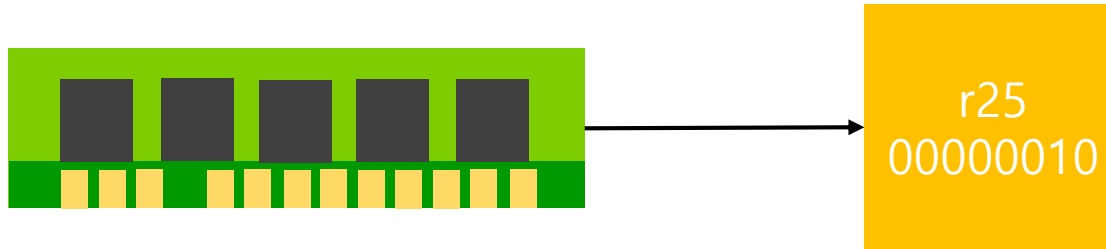
---



- Overwriting Effect in pipeline register
- 연산용 파이프라인 레지스터에 값을 덮어 쓸 경우

# 커플링 현상

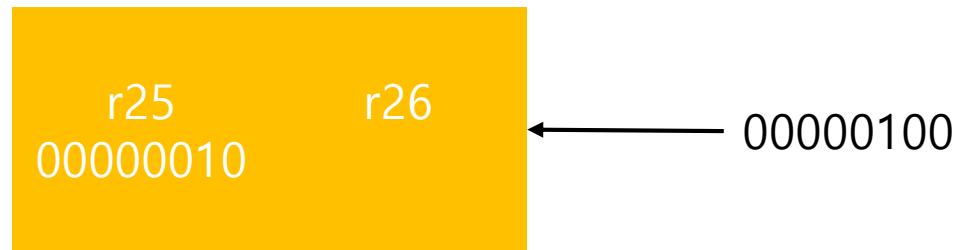
---



- Memory Remnant Effect
- 메모리에서 값을 불러오는 값끼리 영향

# 커플링 현상

---



- Neighbour Leakage Effect
- 인접 레지스터에 값이 저장될 경우



# 연구 진행 현황

---

- 1월: 초동 세미나
- 2월: 코드 분석 및 취약점 파악
- 3월: 논문 작성 마무리 및 제출

# 연구 진행 현황

---

- 구글 스프레드시트의 작업 결과물을 공유
- 공동 작업자: 김경호, 김현준, 최승주
- 팀원들의 협력으로 순조로운 진행을 보임

# 감사합니다

---

2019. 02. 17.