AVR 상에서의 CHAM 128/128 구현

유튜브 주소 : https://youtu.be/79flN61V0BE

AVR

CHAM

CHAM 128/128 구현

AVR

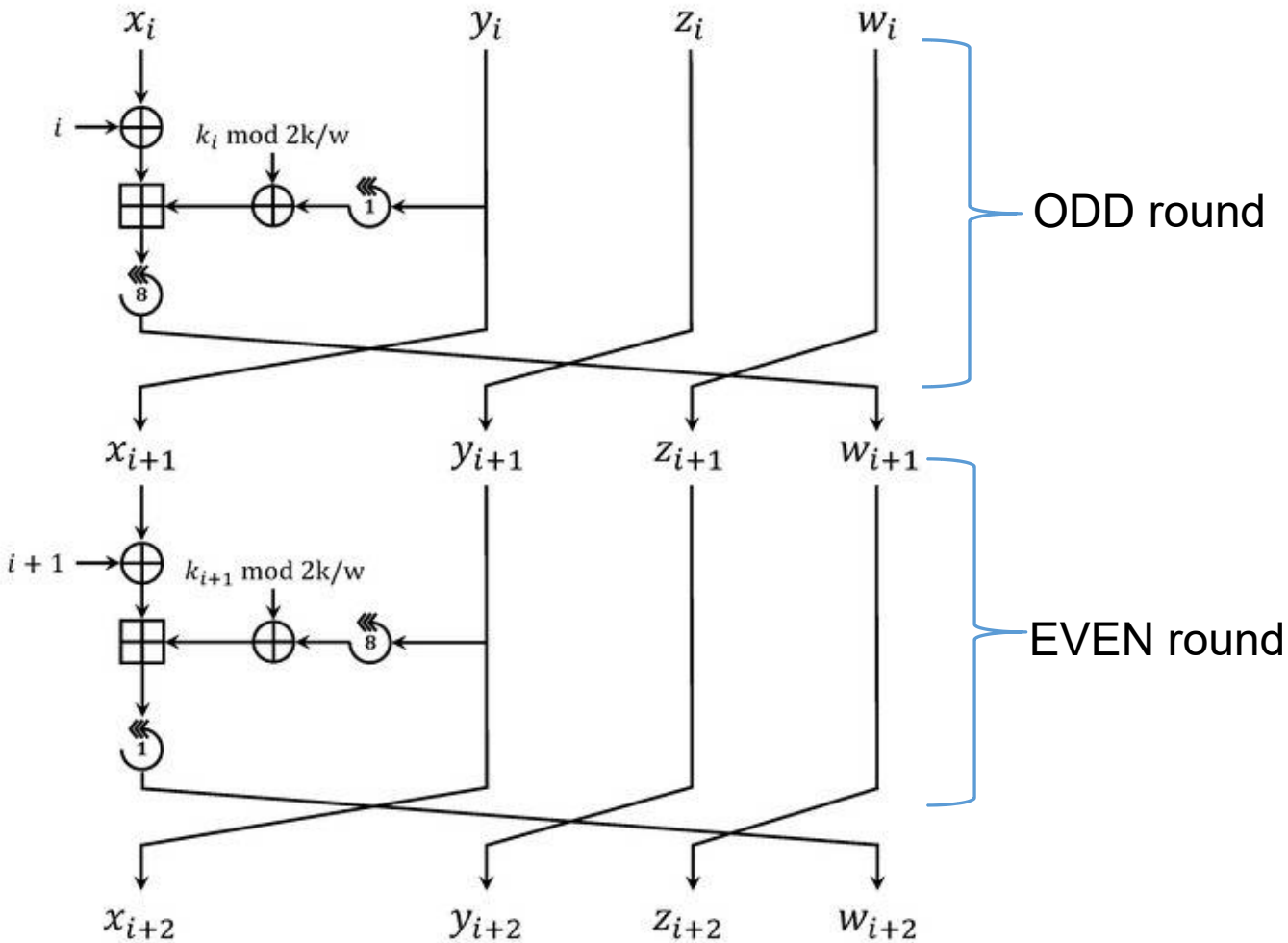
- AVR - Atmel 사의 범용 RISC 마이크로 컨트롤러
- ATmega 128 프로세서
  - 8bit 프로세서
  - 범용 레지스터 - 8bit 32개
    - R1 : zero register
    - R2~R17, R28, R29 : callee saved register
    - R26, R27 : X pointer register
    - R28, R29 : Y pointer register
    - R30, R31 : Z pointer register
    - 매개변수 - (R24,R25), (R22, R23), (R20, R21)... 순서로 입력
    - 포인터 레지스터를 통해 매개변수 활용(MOVW 명령어 사용)

CHAM

- IoT 환경에서 사용되는 것을 목적으로 개발된 국산 경량암호알고리즘

- 세가지 타입 존재
  - 64/128, 128/128, 128/256

- 라운드 횟수
  - 64/128 : 88 round
  - 128/128 : 112 round
  - 128/256 : 120 round



Q & A