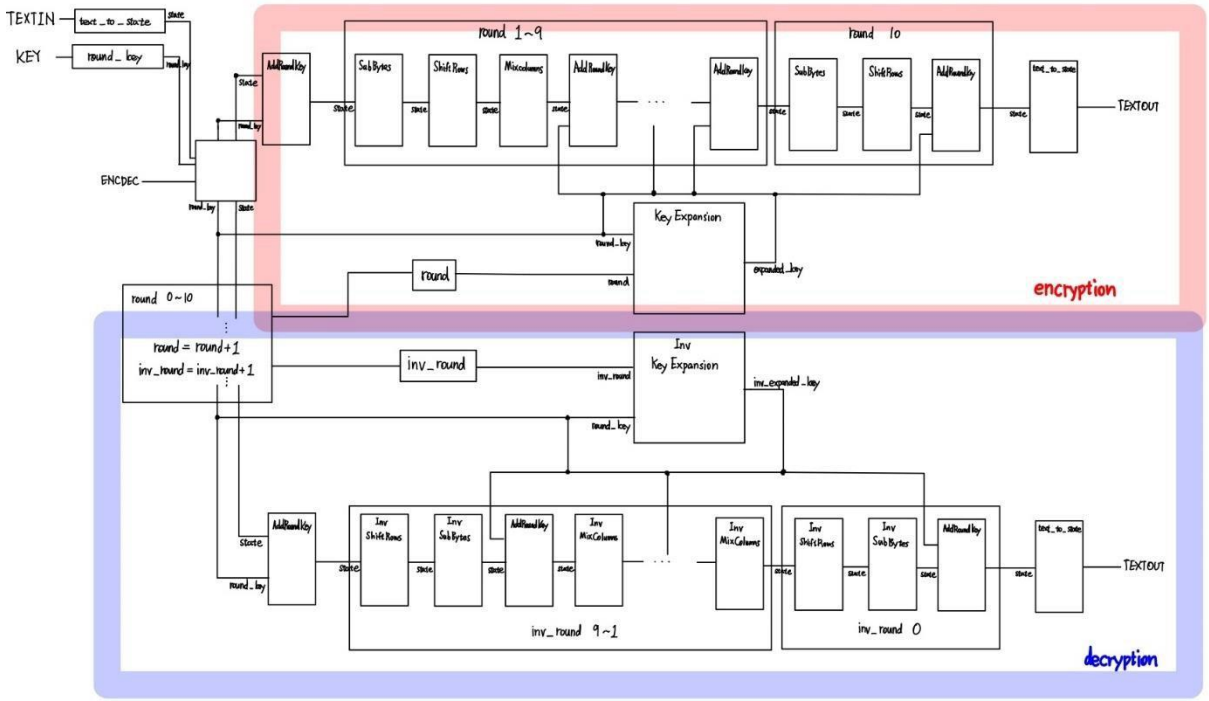
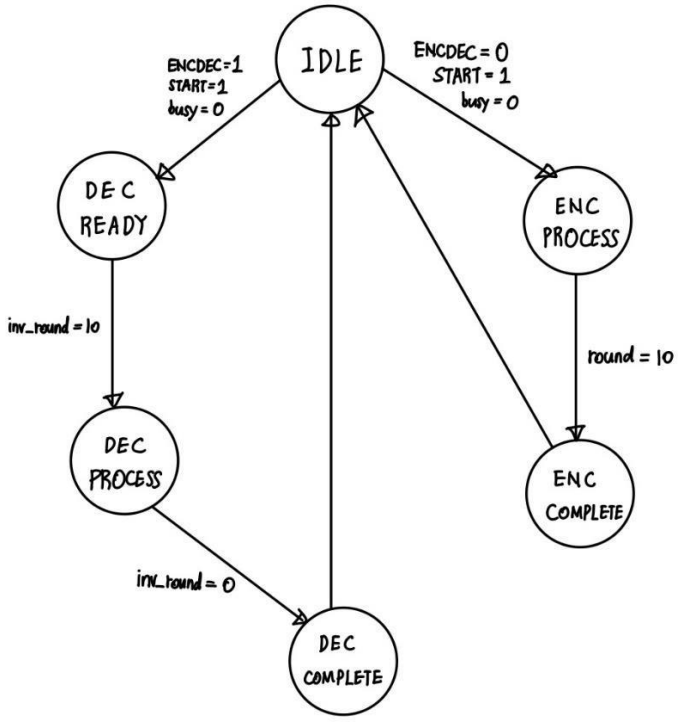
AES Design Report

2023016057 조신근

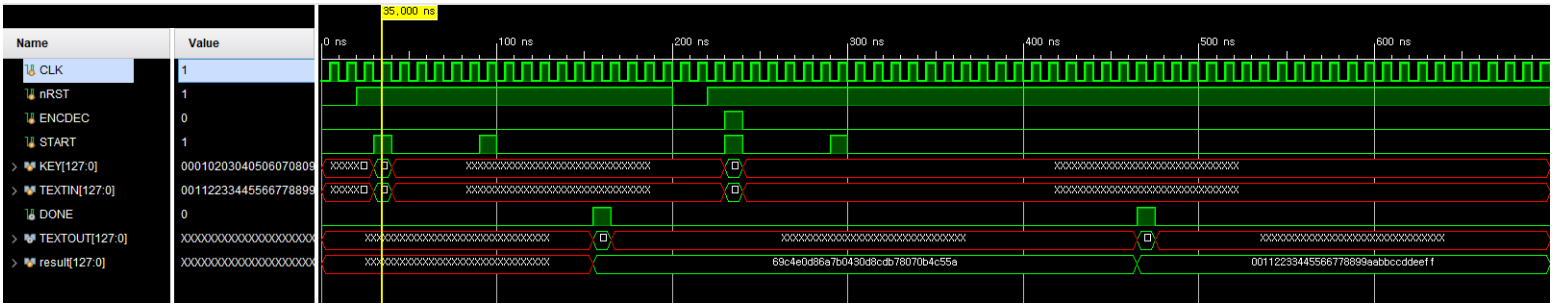
- DataPath



- FSM



- Waveforms



- Source Description

!!) AES알고리즘에서는 state가 열기준으로 저장되었을 때를 기준으로 shiftrows, mixcolumns과 같은 연산들이 진행되므로, plaintext를 열기준으로 state에 저장하여 아래 연산들을 진행함.

1) **신호 설명**:

- state: 현재 AES 상태를 나타내는 128비트 레지스터.
- round: 현재 라운드를 추적하는 5비트 카운터.
- inv_round: 복호화 시 사용하는 라운드 카운터.
- round_key: 현재 라운드에서 사용되는 키.
- sub_bytes_out, shift_rows_out, mix_columns_out, add_round_key_out: AES의 각 단계(SubBytes, ShiftRows, MixColumns, AddRoundKey)의 출력.
- expanded_key, inv_expanded_key: 각 라운드에 확장된 키.
- inv_sub_bytes_out, inv_shift_rows_out, inv_mix_columns_out: 복호화 단계의 출력.

2) **상태 머신 정의**:

- IDLE: 대기 상태.
- ENC_PROCESS: 암호화 처리 중.
- ENC_COMPLETE: 암호화 완료.
- DEC_READY: 복호화 준비 중.
- DEC_PROCESS: 복호화 처리 중.
- DEC_COMPLETE: 복호화 완료.

3) **레지스터**:

- current_state, next_state: 현재 상태와 다음 상태를 저장.

- !) state와 current_state, next_state는 완전 다름. state는 뒤에 쓰일 연산에 사용되는 배열을 뜻함.
- round_key_next: 다음 라운드 키.
- is_DEC: 복호화 모드 여부.
- busy: 연산 중 여부를 나타내는 플래그.

4) **서브 모듈 설명**:

- SubBytes: 8비트 단위로 Sbox연산.
- ShiftRows: Row 1은 한 칸, Row 2는 두 칸, Row 3은 3칸 왼쪽으로 비트 이동.
- MixColumns: Galois Field 곱셈 함수 (gmul)를 이용해서 주어진 배열에 맞게 행열 곱을 Galois Field에 따라 수행.
- KeyExpansion: round와 round_key를 이용해 다음 round에 쓰일 expanded_key를 추출..
- InvShiftRows, InvSubBytes, InvMixColumns, InvKeyExpansion: 복호화 단계의 각 대응 모듈.
- AddRoundKey: 라운드 키를 현재 state에 xor연산.

!) **AddRoundKey 모듈의 data_in 입력**:

- 암호화(is_DEC == 0)일 때:
    - 첫 라운드(round == 0): state.
    - 마지막 라운드(round == 10): shift_rows_out (MixColumns 생략).
    - 그 외 라운드: mix_columns_out.
- 복호화(is_DEC == 1)일 때:
    - 첫 라운드(inv_round == 10): state.
    - 그 외 라운드: inv_sub_bytes_out.

5) **리셋 조건 (!nRST)**:

- 상태를 IDLE로 초기화.

- round, DONE, busy를 초기값으로 설정.

6) **상태 전이 및 동작**:

- **IDLE 상태**:
  - START 신호가 활성화되고 busy가 아닐 때:
    - round_key를 입력 KEY로 설정.
    - TEXTIN을 내부 state로 변환 (text_to_state 함수 사용).
    - is_DEC를 ENCDEC 값으로 설정 (암호화 또는 복호화 모드 선택).
    - busy 플래그를 1로 설정.
  - 출력 TEXTOUT을 미정(unknown) 상태로 설정.
  - round, inv_round를 0으로 초기화.
  - DONE을 0으로 설정.
- **ENC_PROCESS 상태**:
  - **첫 번째 라운드 (round == 0)**:
    - AddRoundKey 단계 수행.
    - state를 add_round_key_out으로 업데이트.
    - round를 증가.
    - round_key를 expanded_key로 업데이트.
  - **중간 라운드 (round < 10)**:
    - 순차적으로 SubBytes, ShiftRows, MixColumns, AddRoundKey 단계 수행.
    - state를 각 단계의 출력으로 업데이트.
    - round와 round_key를 업데이트.
  - **마지막 라운드 (round == 10)**:
    - MixColumns 단계를 생략하고 SubBytes, ShiftRows, AddRoundKey 단계 수행.
    - state를 각 단계의 출력으로 업데이트.

        - round를 0으로 초기화.
        - round_key를 expanded_key로 업데이트.

- **ENC_COMPLETE 상태**:
    - 최종 state를 TEXTOUT으로 변환하여 출력.
    - DONE 신호를 1로 설정.
    - busy 플래그를 0으로 해제.
- **DEC_READY 상태**:
    - inv_round가 10 미만일 때:
        - round와 inv_round를 증가.
        - round_key를 expanded_key로 업데이트.
- **DEC_PROCESS 상태**:
    - **첫 번째 라운드 (inv_round == 10)**:
        - AddRoundKey 단계 수행.
        - state를 add_round_key_out으로 업데이트.
        - round를 증가.
        - inv_round를 감소.
        - round_key를 inv_expanded_key로 업데이트.
    - **중간 라운드 (0 < inv_round < 10)**:
        - InvShiftRows, InvSubBytes, AddRoundKey, InvMixColumns 단계 순차 수행.
        - state를 각 단계의 출력으로 업데이트.
        - round를 증가.
        - inv_round를 감소.
        - round_key를 inv_expanded_key로 업데이트.
    - **마지막 라운드 (inv_round == 0)**:

        - InvShiftRows, InvSubBytes, AddRoundKey 단계 수행.
        - state를 각 단계의 출력으로 업데이트.
- **DEC_COMPLETE 상태**:
    - 최종 state를 TEXTOUT으로 변환하여 출력.
    - DONE 신호를 1로 설정.
    - busy 플래그를 0으로 해제.

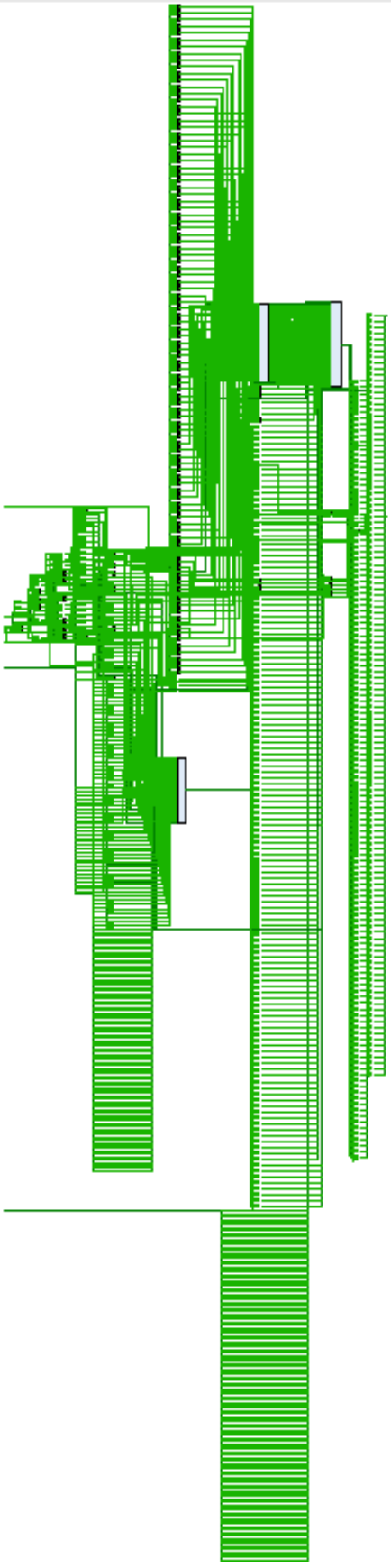
7) 상태 전이 규칙:

- **IDLE**:
    - 암호화 모드(ENCDEC == 0)이고 START 신호가 활성화되며 busy가 아닐 경우 ENC_PROCESS로 전이.
    - 복호화 모드(ENCDEC == 1)이고 START 신호가 활성화되며 busy가 아닐 경우 DEC_READY로 전이.
- **ENC_PROCESS**:
    - round가 10일 경우 ENC_COMPLETE로 전이.
- **ENC_COMPLETE**:
    - 항상 IDLE로 전이.
- **DEC_READY**:
    - inv_round가 10일 경우 DEC_PROCESS로 전이.
- **DEC_PROCESS**:
    - inv_round가 0일 경우 DEC_COMPLETE로 전이.
- **DEC_COMPLETE**:
    - 항상 IDLE로 전이.

8) text_to_state 함수

- 입력된 128비트 텍스트(TEXTIN 또는 state)를 내부 state 배열 형식으로 변환하거나 그 반대로 변환하기 위해 열기준으로 저장 후 반환.

- Synthesis



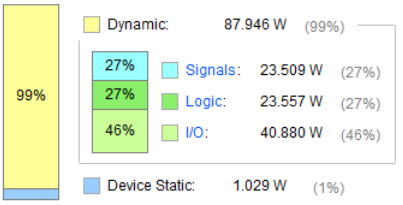
Summary

Power estimation from Synthesized netlist. Activity derived from constraints files, simulation files or vectorless analysis. Note: these early estimates can change after implementation.

Total On-Chip Power:	**88.975 W (Junction temp exceeded!)**
Design Power Budget:	**Not Specified**
Power Budget Margin:	**N/A**
Junction Temperature:	**125.0°C**
Thermal Margin:	-107.5°C (-56.4 W)
Effective ϑJA:	1.9°C/W
Power supplied to off-chip devices:	0 W
Confidence level:	Low

Launch Power Constraint Advisor to find and fix invalid switching activity

On-Chip Power



Check Timing

Timing Check	Count	Worst Severity
unconstrained_internal_endpoints	807	High
no_clock	441	High
no_input_delay	259	High
no_output_delay	129	High
constant_clock	0	
pulse_width_clock	0	
multiple_clock	0	
generated_clocks	0	
loops	0	
partial_input_delay	0	
partial_output_delay	0	
latch_loops	0	