BLAKE-512 Hardware Datasheet

Description

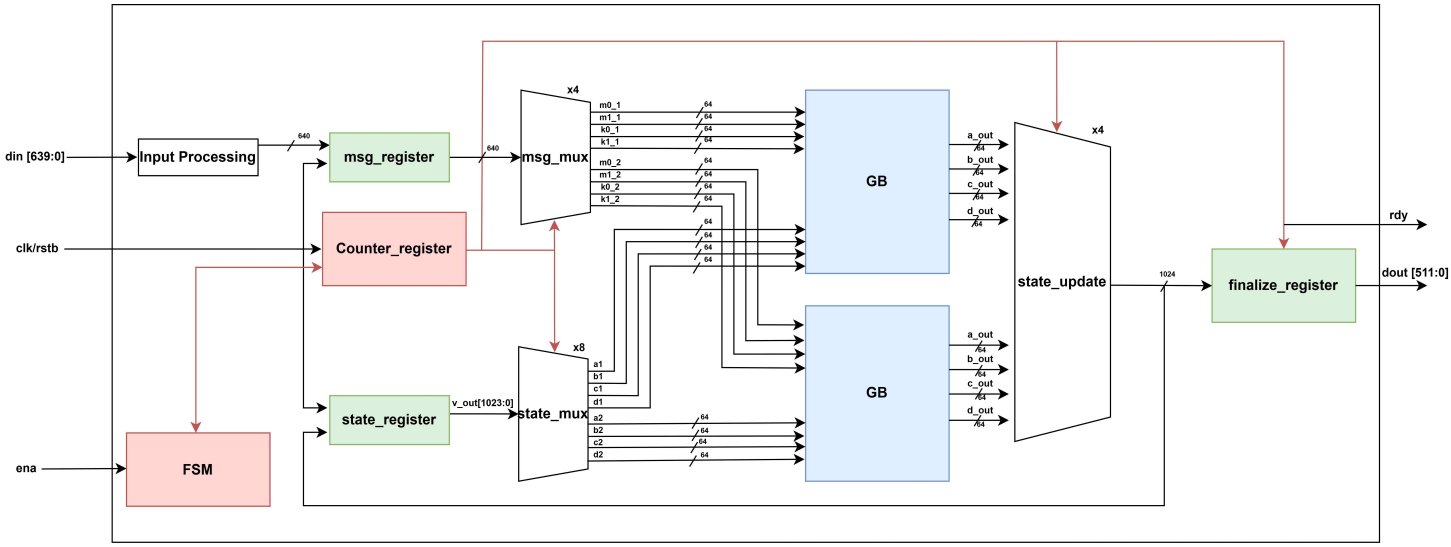
1. **기능** : 640bit의 메시지 블록을 입력으로 받아 512-bit의 고정된 암호화된 값을 생성하는 하드웨어 모듈
2. **구조** : FSM기반 컨트롤러와 64라운드의 연산을 수행하는 Datapath로 구성됨.

Performance

1. **input** : ena신호와 동기화 되어 64cycle주기로 연속적인 데이터 주입 가능
2. **Latency** : 데이터 입력 후 출력 생성까지 64cycle소모.

BLAKE-512 Hardware Datasheet

1. Block Diagram



[figure 1.1 BLAKE block diagram]

Input processing

640비트 입력 데이터를 32비트 단위로 분할한 후, 각 32비트 워드의 바이트 순서를 뒤집어 출력한다.

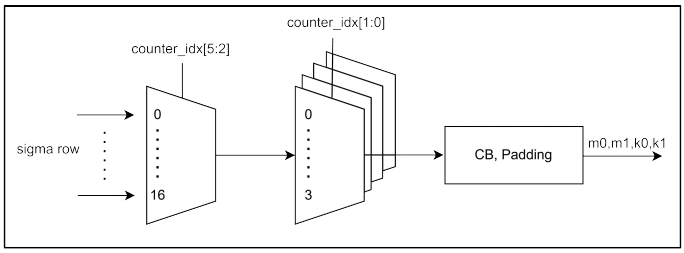
msg_register

초기화 상태에서 바이트 스왑된 640비트 입력 메시지를 내부 레지스터에 저장하며, 이후 신호에 따라 내부 라운드 연산이 수행되기 전 데이터 제공 및 연산 동안 저장된 값을 유지한다.

state_register

BLAKE 알고리즘의 초기 상수값(IV512)을 내부 레지스터에 로드한 후, 라운드가 진행될 때마다 1024비트 내부 상태 변수(v0~ v15)를 유지하고 업데이트한다.

msg_mux



메시지 레지스터에서 전달된 입력 데이터는 시그마 행렬 규칙에 따라 처리되며, 내부 패딩 로직을 통해 1024비트 메시지 블록으로 확장된다. counter_idx[5:2]는 라운드별 시그마 행 선택에 사용되며, counter_idx[1:0]은 Column 및 Diagonal 연산에 필요한 메시지 워드 및 상수(CB) 인덱스를 생성하여 G-함수 코어에 m0, m1, k0, k1입력으로 제공한다.

GB

덧셈, XOR 및 순환 회전 연산의 조합을 통해 데이터를 압축하고 혼합하는 기능을 수행한다.

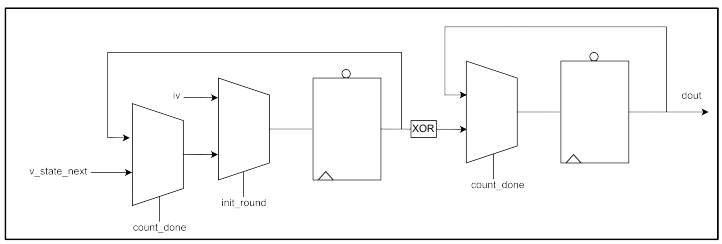
State_mux

Column 및 Diagonal 처리 단계에 따라 1024비트 내부 상태 레지스터에서 출력된 데이터를 비트 슬라이싱하여 a, b, c, d 상태 변수 집합을 생성하고, 이를 멀티플렉싱하여 두 개의 GB-함수 모듈에 공급한다.

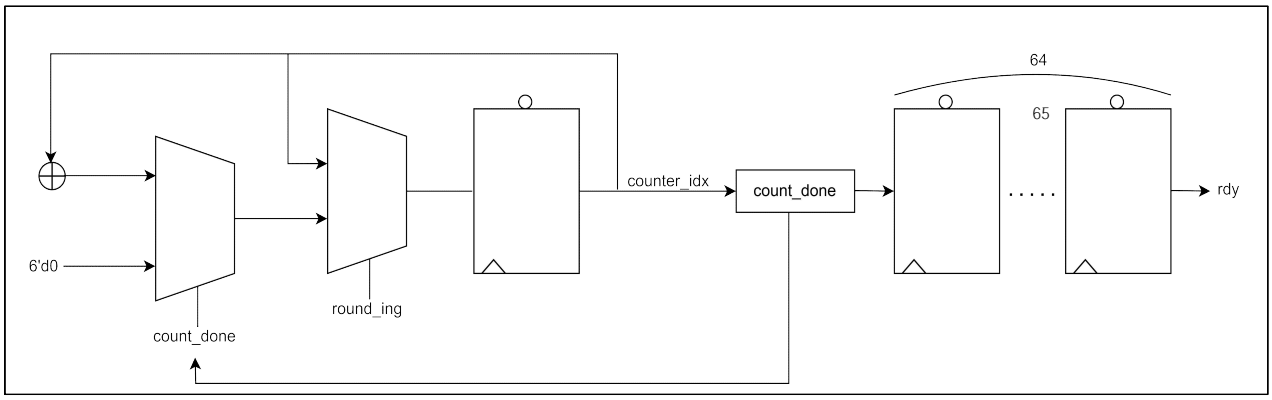
State_update

현재 단계에 따라 GB함수에서 계산된 출력 값(a, b, c, d)을 내부 상태 변수에 반영함으로써, 다음 연산을 위한 1024비트 내부 상태 벡터를 생성한다.

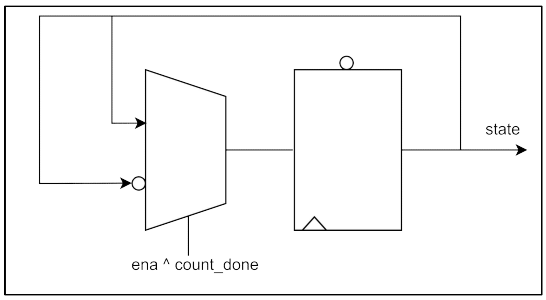
final_register



모든 라운드 처리가 종료된 이후 내부 상태 변수와 이전 해시 값의 XOR 연산을 통해 최종 512비트 출력 값(dout)을 생성한다.



[figure 1.2 Counter_register Diagram]



[figure 1.3 FSM Diagram]

Counter register 블록에서 생성되는 count_done신호(카운트 인덱스 = 64)와 controller 모듈의 state 신호는 상호 연동되어 동작하며, 본 설계는 두 개의 FSM이 상호 제어하는 구조로 구성된다.

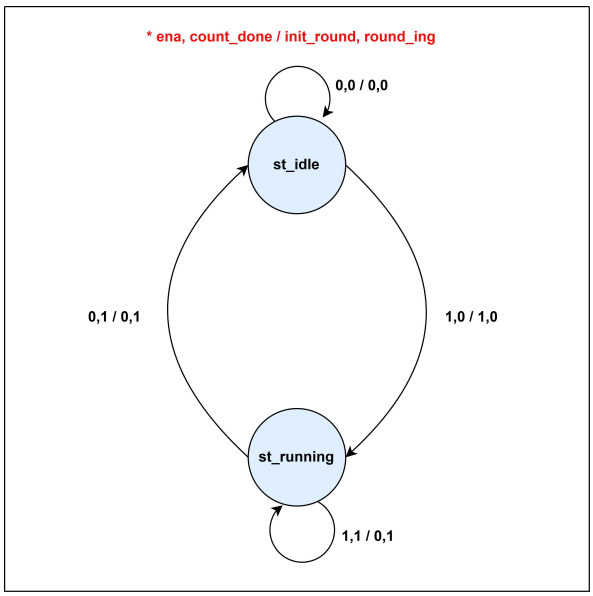
counter_register

해당 모듈은 최대 64번의 연산을 카운트하고, 카운트 인덱스를 이용하여 state_muxmsg_mux의 선택 신호를 제어한다. rdy신호는 카운트 종료 이후 시프트 레지스터를 통해 지연되어, 128번째 클록 사이클에서 활성화된다.

FSM

FSM 블록은 initial state와 round state의 두 가지 상태로 구성된다.
initial state는 입력이 인가되지 않은 초기 기본 상태 또는 64사이클 연산 완료 후 다음 입력을 대기하는 상태이며, round state는 해시 연산이 진행 중인 상태를 나타낸다. 64사이클의 연산이 종료되면 FSM은 다시 initial state로 복귀한다. 각 FSM 블록에서 생성된 제어 신호는 BLAKE 레지스터 블록에 전달되어 내부 연산을 제어한다.

2. State Diagram



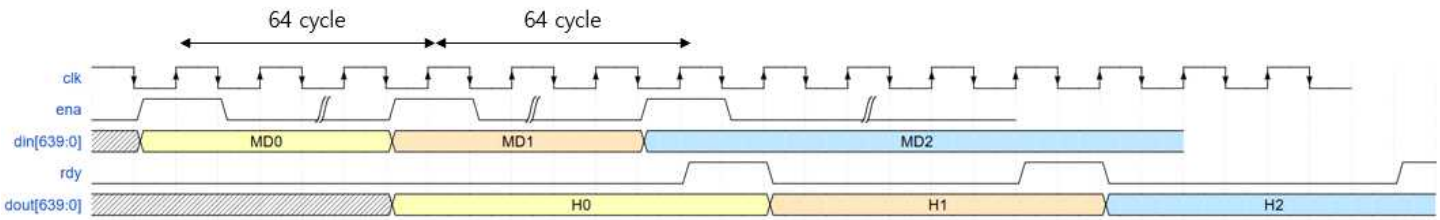
[figure 2.1 State Diagram]

State	Condition to Exit	Output	Description
st_idle	ena = 1	init_round = 1	연산 준비 및 초기 데이터 로드
st_running	count_done = 1	rounding = 1	64라운드 연산 진행

[figure 2.2 BLAKE state]

1. 시작 시점: ena 신호가 '1'이 되는 순간, init_round가 1이 되면서 input data를 가져오게 된다.
2. 연산 중: 그와 동시에 상태는 바로 st_running으로 바뀌고 Datapath에 round_ing 신호를 계속 보내준다.
3. 종료 시점: 64라운드 계산이 다 끝나 카운터가 count_done 신호를 쏴주면, Controller는 다시 st_idle로 돌아가게 된다.

3. Timing Diagram



- Input : ena 신호에 맞춰 64사이클 주기로 데이터가 연속해서 들어온다.
- Output: 연산이 끝나면 rdy 신호가 High가 되면서 512비트 해시값(dout)을 출력한다.
- Latency : 각 데이터는 입력된 시점부터 정확히 128사이클 뒤에 출력이 완료된다. 하지만 연산 자체는 64사이클에 완성됨으로 rdy 발생 신호를 수정하여 latency를 줄일 수 있다.