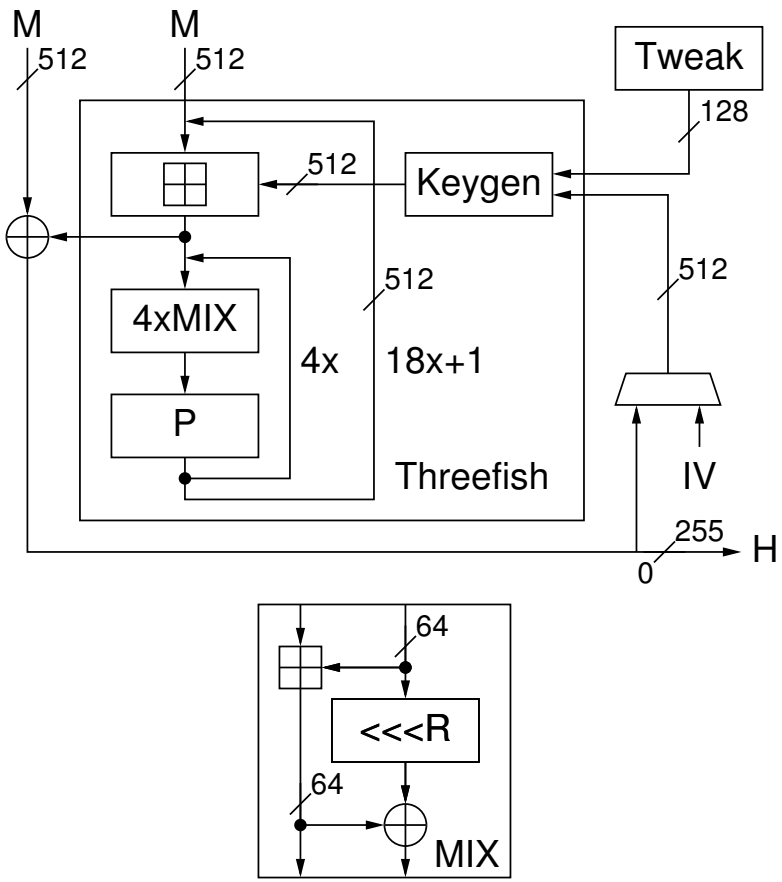
Skein Algorithm

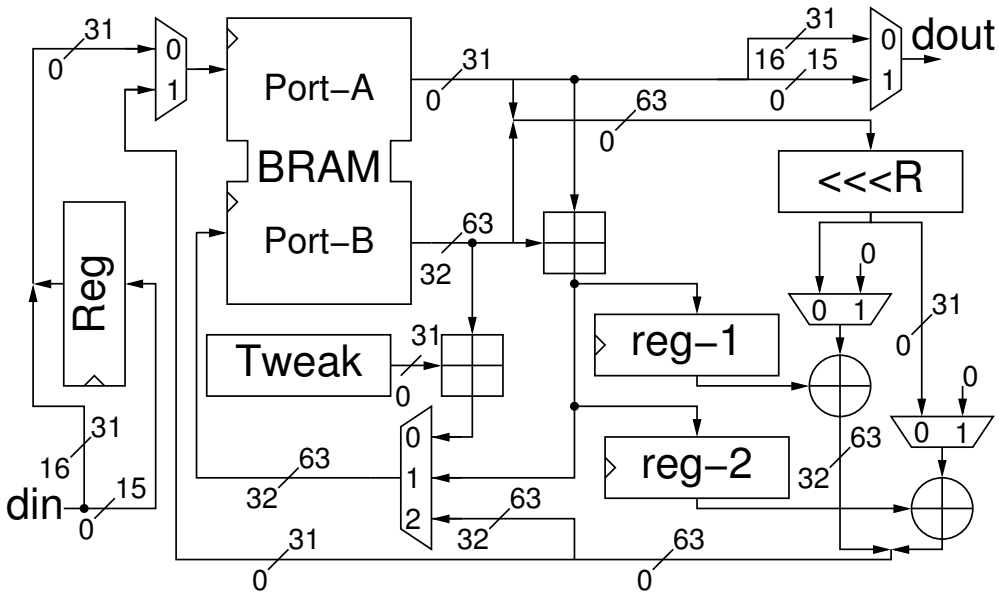


- 64-bit adders lead to long delay.
- Algorithm cannot be folded.

Memory Requirements: 2,112 bits

- State: 512 bits
- Processed IV: 512 bits
- Message: 512 bits
- Rotation Tweak Constants: 64 bit
- Hash Chaining Value: 512 bits

Skein Implementation BRAM

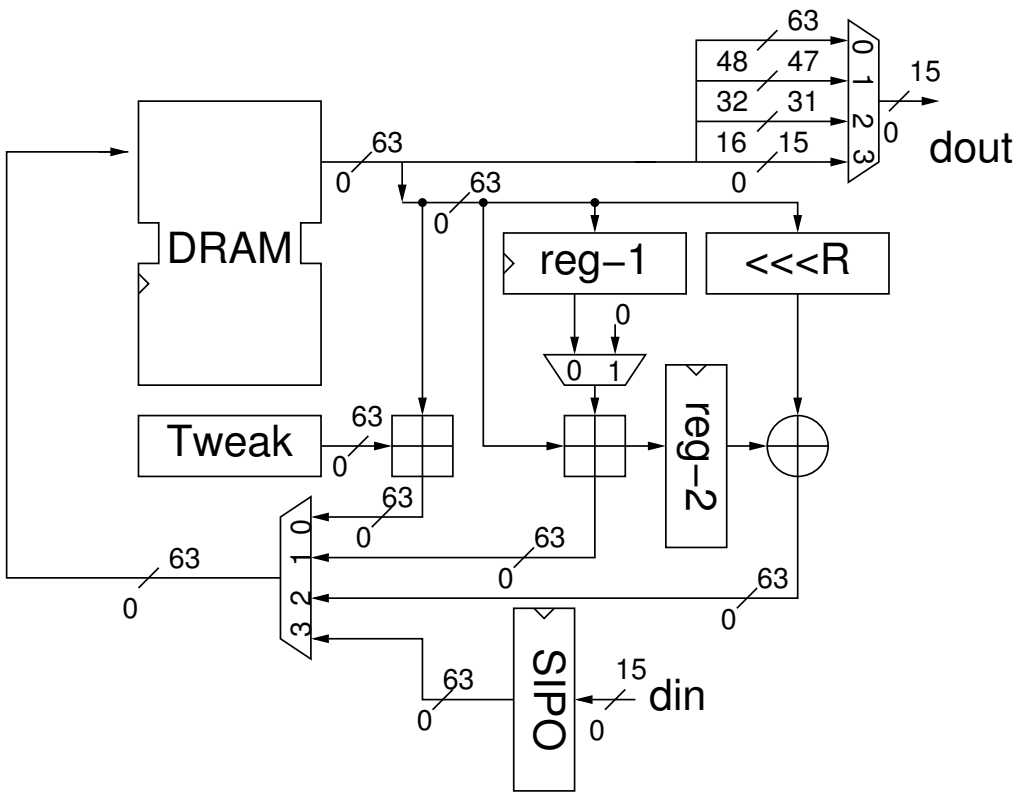


Performance (Clock Cycles)

- Initialization: 5
- Loading: 32
- MIX: 18x4x20=1440
- Keygen: 19x45+3=858
- Permutations: 109
- Total per Block: 2407

- Using 32-bit adder to reduce critical path (no clk penalty).
- Barrel shifter is single largest block in the design (192 slices).
- Finalization takes as many clock cycles as 1 block hash.
- **Scalability:** Running Keygen and MIX in parallel.

Skein Implementation Logic Only

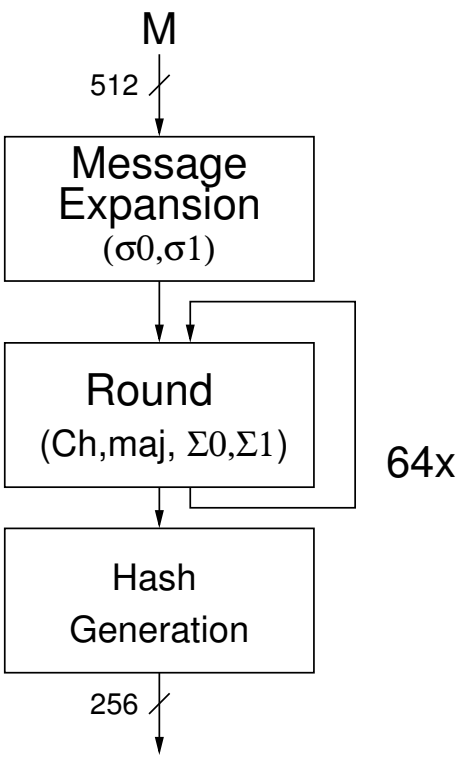


Performance (Clock Cycles)

- Initialization: 5
- Loading: 32
- MIX: 18x4x20=1440
- Keygen: 19x47+1=894
- Permutations: 32
- Total per Block: 2366

- Have to use 64-bit, else need dualport Distributed RAM at 356 slices (from 162).
- Larger adder increases length of critical path.

SHA-2 Algorithm

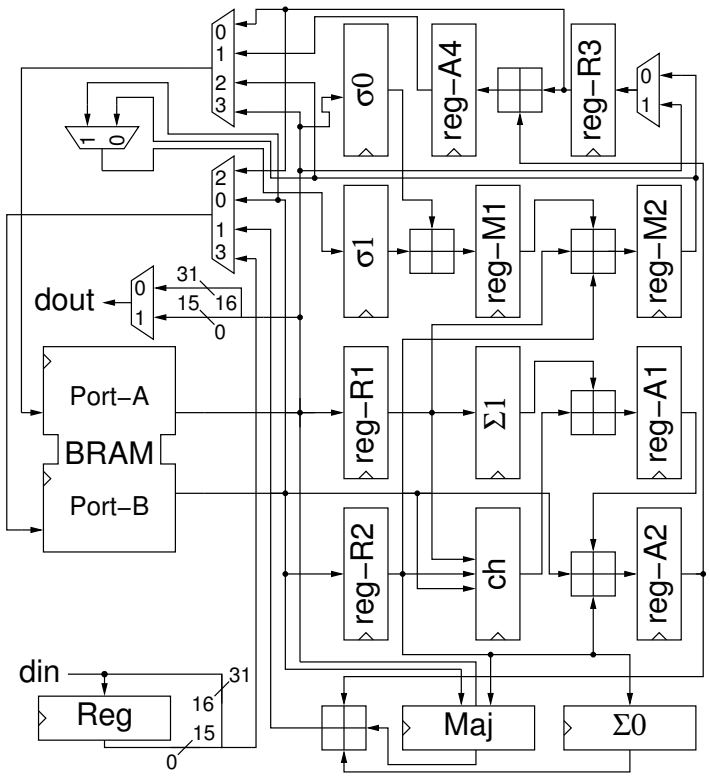


- Uses six logic functions *Ch*, *Maj*, Σ0, *Sigma*1, *sigma*0, and *sigma*1.
- Algorithm cannot be folded.

Memory Requirements: 3,072 bits

- State: 512 bits
- Constants:64x32=2,048 bits
- Hash values: 2x8x32=512 bits

SHA-2 Implementation BRAM

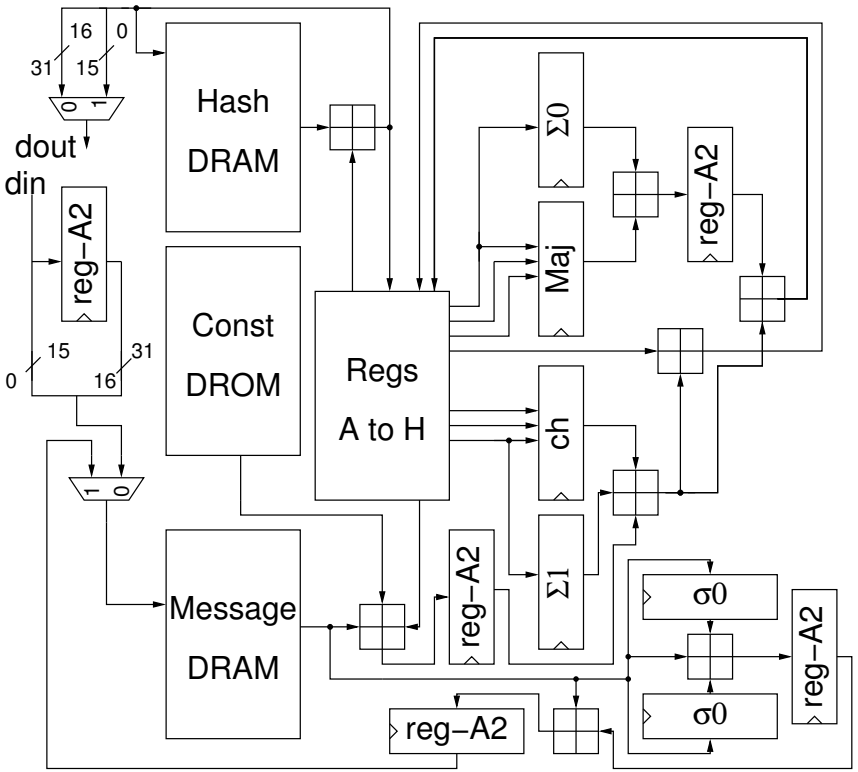


Performance (Clock Cycles)

- Initialization: 2
- Loading: 32
- Message expansion=99
- Round: 64x7=448
- Hash generation: 16
- Total per Block: 563

- BRAM contains constants, message, working variables and intermediate hash.
- Quasi-pipelined the round operation.

SHA-2 Implementation Logic Only



Performance (Clock Cycles)

- Initialization: 2
- Loading: 32
- Message expansion=196
- Round: 64x3=192
- Hash generation: 16
- Total per Block: 404

- Constants, message and intermediate hash are stored in DRAMs and working variable in registers.
- Use of registers for working variable reduced the number of clock cycles per round.