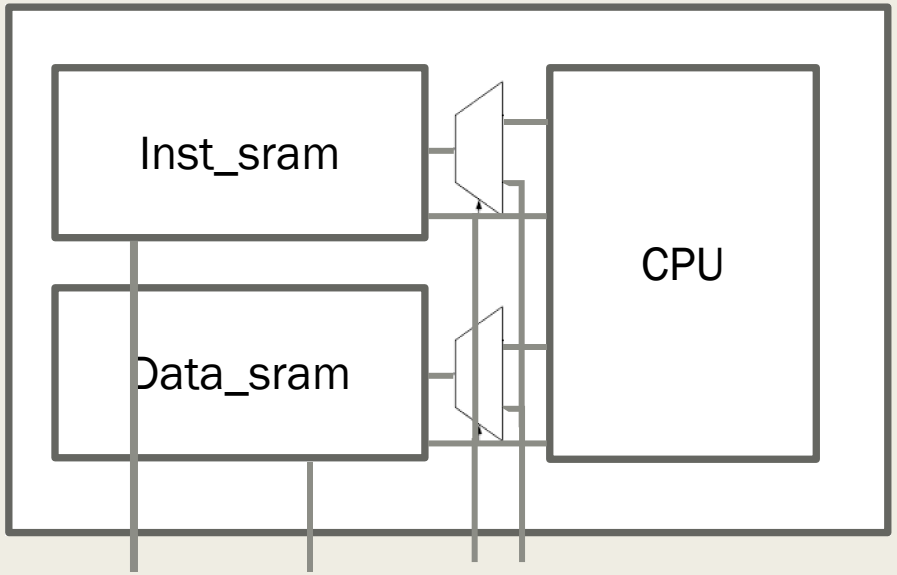
8/12 MEETING

Outline

1. Merge sram_512x8 into processor.
2. Implement AES on basic processor.
3. Overhead analysis.
4. Latency analysis.

Hierarchy of processor

- RISC-V
  - *CPU*
  - *Instruction_memory (2KB, 4KB)*
  - *Data_memory (2KB)*

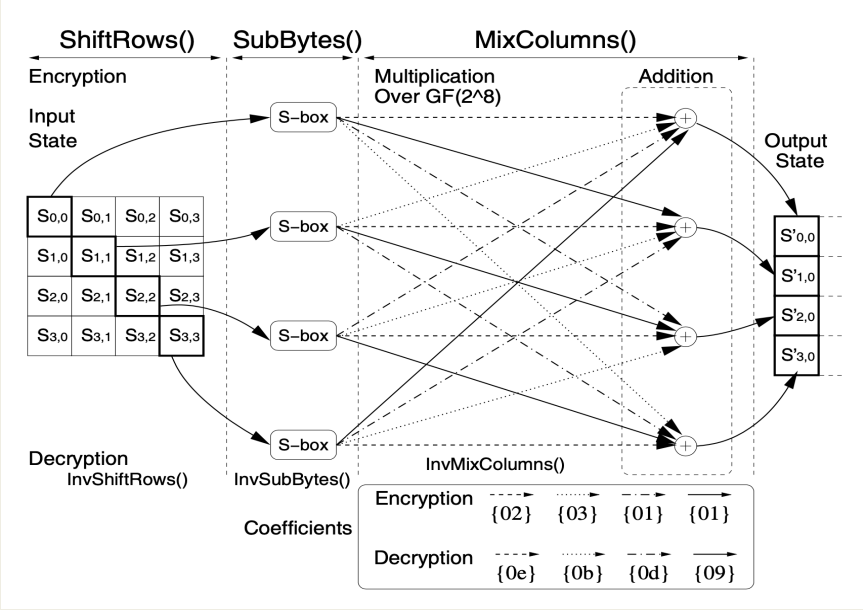


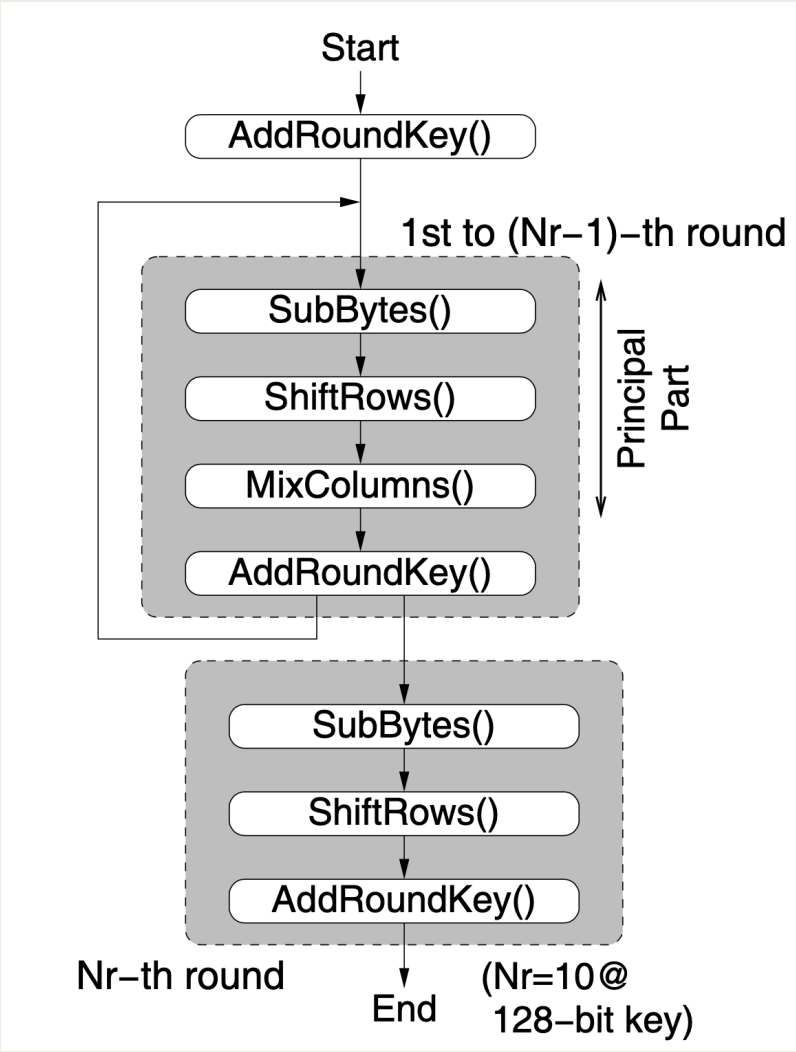
Implement AES

- Compute-oriented
  - Online computation, less memory
  - Substitute: pre-compute S-BOX /xtime, less latency
- Table-oriented
  - Offline pre-computation, less latency but increasing memory
  - Column-packed
- Bit-sliced
  - Avoid timing attacks on processors with cache memory due to table look-ups.

AES (advanced encryption standard)

- AES-128/192/256:
  - Plain text : 128bits (16 bytes)
  - Key : 128/192/256bits
  - Rounds : 10/12/14
  - Cypher : 128bits (16 bytes)





Base vs ISE

	ISE	Base
Sbox method	Offline computation	Look-up table
Sbox implement	262 nand gate equivalent	512 bytes
Encrypt	20 (inst/round)	314 (inst/round)
Decrypt	20 (inst/round)	618 (inst/round)
Stored instruction(enc/dec)	121/146 lines (x4 bytes)	419/525 lines (x4bytes)
Stored data	72 bytes	584 bytes

Area overhead

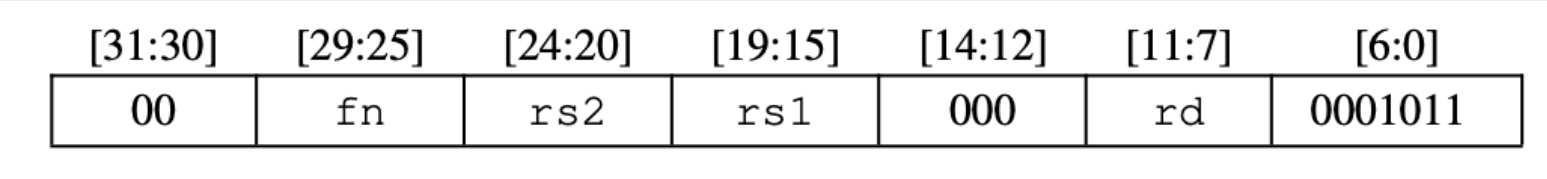
	ISE (2KB*2 sram)	ISE (4KB+2KB sram)	Base (4KB+2KB sram)
Cycle time	7.5 ns	7.6 ns	7.5 ns
Combination	14280 nand eq	14300 nand eq	13267 nand eq
Non-combination	14607 nand eq	14895 nand eq	14841 nand eq
memory	48520 nand eq	72930 nand eq	72930 nand eq
Total (without memory)	28888 nand eq	29196 nand eq	28109 nand eq

Time latency

	ISE (2KB*2 sram)	ISE (4KB+2KB sram)	Base (4KB+2KB sram)
Cycle time	7.5 ns	7.6 ns	7.5 ns
Encrypt cycle	487	487	4413
Decrypt cycle	1044	1044	16492
Enc/dec time	3.652/7.83 us	3.701/7.934 us	33.097/123.69 us
Enc/dec time (with loading data)	9.428/13.605 us	11.5/15.732 us	40.792/131.385 us

Hardware-assisted T-table

- https://github.com/mjosaarinen/lwaes_isa
- Add 4 instructions (2 for encryption, 2 for decryption)
- Encryption requires 20 instructions/round (4 lw, 16 saes.v3.encsm)



[31:30]	[29:25]	[24:20]	[19:15]	[14:12]	[11:7]	[6:0]
00	fn	rs2	rs1	000	rd	0001011

- fn [1:0]: select a single byte from rs2.
- fn [4:2]: specify saes32.encsm/saes32.encs/saes32.decsm/saes32.decs
- rs1: store round key
- rs2: store cypher
- rs1=rd