8/26 MEETING

Outline

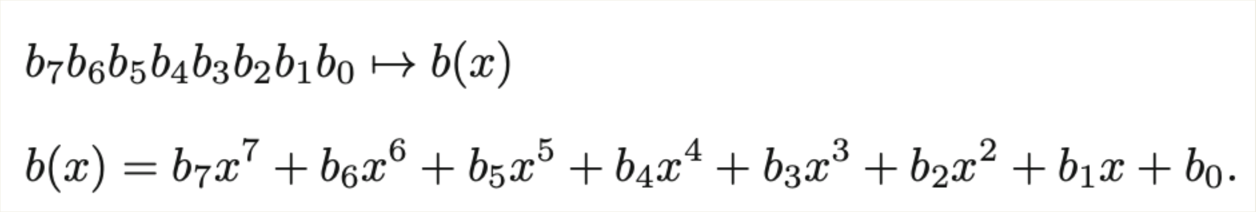
1. RISCV-M standard extension
2. AES software acceleration(for base CPU)
3. Compare base and ISE
4. AES core (accelerator)

RISC-V M standard extension

- Previous
  - *32 cycles per operation*
  - *13511 um^2 (0.13um process)*
- Modified
  - *Instance Design Ware*
  - *2 cycles per operation*
  - *55581 um^2 (0.13um process)*

Correction

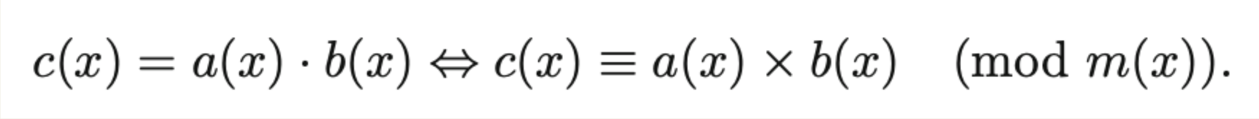
- Don’t need multiplication in AES
- Polynomial over finite field



$$b_7b_6b_5b_4b_3b_2b_1b_0 \mapsto b(x)$$

$$b(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0.$$

  - *Addition : XOR*
  - *Multiplication*



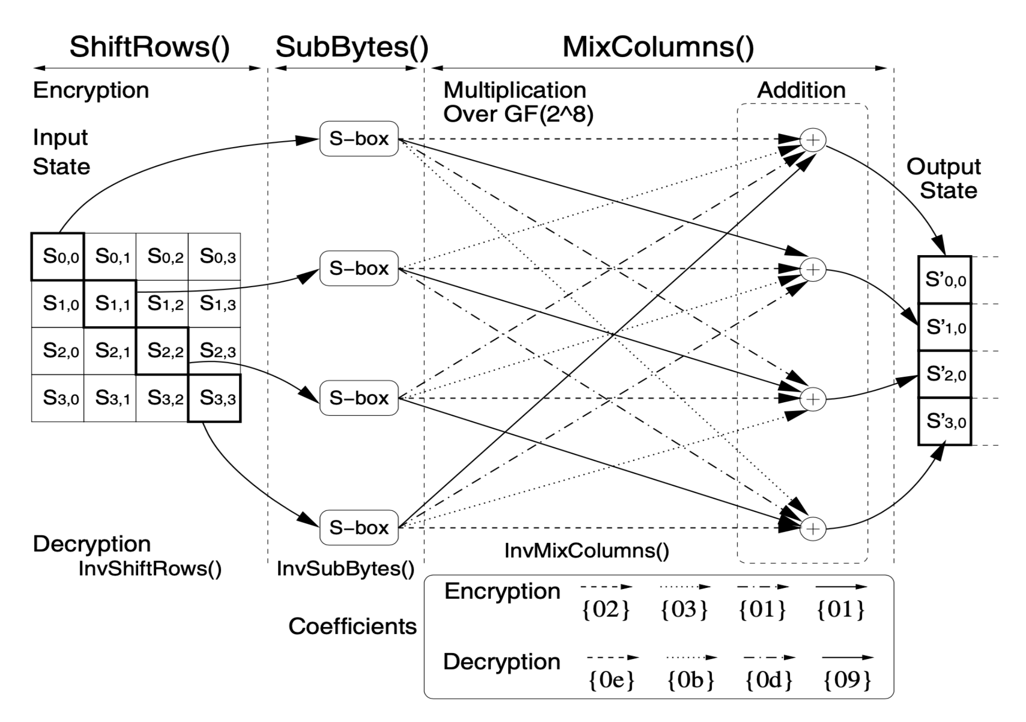
$$c(x) = a(x) \cdot b(x) \Leftrightarrow c(x) \equiv a(x) \times b(x) \pmod{m(x)}.$$

Time latency (review)

	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

AES software acceleration (for base CPU)

1. Table-oriented
2. Combined shift-and-mask instructions
3. Scaled-index loads
4. Byte loads (lbu..)
5. ….


ShiftRows()
SubBytes()
MixColumns()
Encryption
Multiplication Over GF(2^8)
Addition
Input State
Output State
S–box
S–box
S–box
S–box
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S'_{0,0}$
$S'_{1,0}$
$S'_{2,0}$
$S'_{3,0}$
Decryption
InvShiftRows()
InvSubBytes()
InvMixColumns()
Coefficients
Encryption {02} {03} {01} {01}
Decryption {0e} {0b} {0d} {09}

(Efficient Cryptography on the RISC-V Architecture, K. Stoffelen, 2019.09)

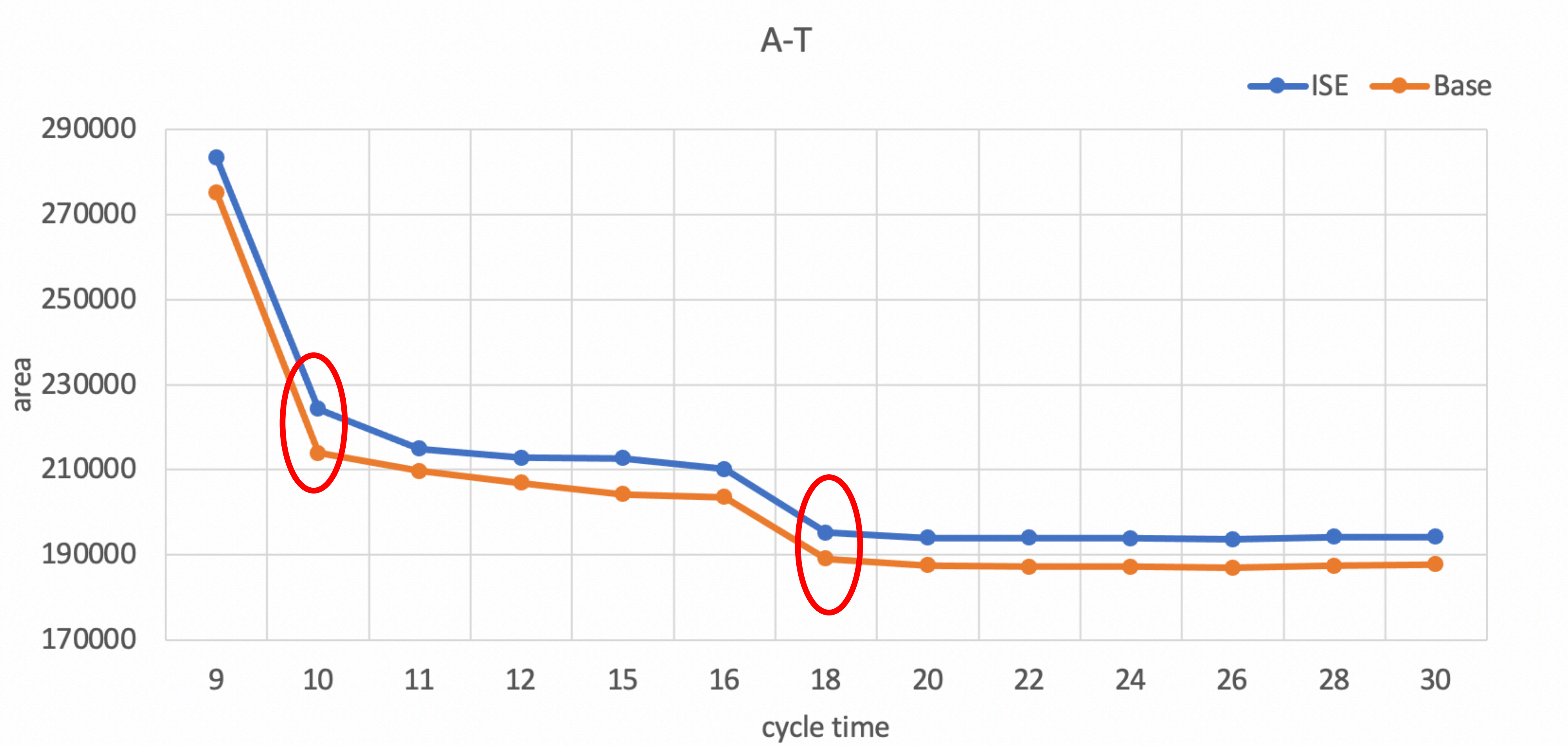
Analysis

- Choose design (A-T analysis)
- Area overhead
- Software memory footprint
- Execute time comparison

Hardware in paper

	SCARV	Rocket
RV32IMC	✓	✓
RV64IMC	x	✓
Pipeline	5	5
Branch prediction	x	✓
Instruciton/data cache	x	✓
Pick	✓	x

A-T analysis


A-T
ISE
Base
290000
270000
250000
230000
210000
190000
170000
area
9
10
11
12
15
16
18
20
22
24
26
28
30
cycle time

Area overhead

	Base	ISE	Base	ISE	SCARV	SCARV-ISE
synthesis	.13um	.13um	.13um	.13um	Yosys	Yosys
Cycle time	10ns	10ns	18ns	18ns	X	X
Area	41998	44023 (x1.048)	37136	38328 (x1.032)	37325	38546 (x1.033)
ISE area	0	1161	0	1161	0	1149

unit : nand gate eq (ps: 1 nand gate = 5.0922 um^2)

Software memory footprint

	Base	ISE	SCARV	SCARV-ISE
Enc-KeyExp	148	86	154	86
Enc	808	290	804	290
Enc total	956	376 (-61%)	958	376 (-61%)
Dec-KeyExp	456	64	174	64
Dec	1508	290	804	290
Dec total	1964	354 (-82%)	978	354 (-64%)
.data	4114	10 (-99%)	5120	10 (-99%)

unit : byte

Execute time comparison

	Base	ISE	SCARV	SCARV-ISE
Enc-KeyExp	389 (29%)	237 (49%)	515 (34%)	312 (52%)
Enc	955 (71%)	250 (51%)	1016 (66%)	291 (48%)
Enc total	1344	487 (-64%)	1531	603 (-60%)
Dec-KeyExp	9161 (56%)	793 (76%)	2307 (69%)	1118 (80%)
Dec	7330 (44%)	251 (24%)	1037 (31%)	286 (20%)
Dec total	16491	1044 (-93%)	3344	1404 (-58%)

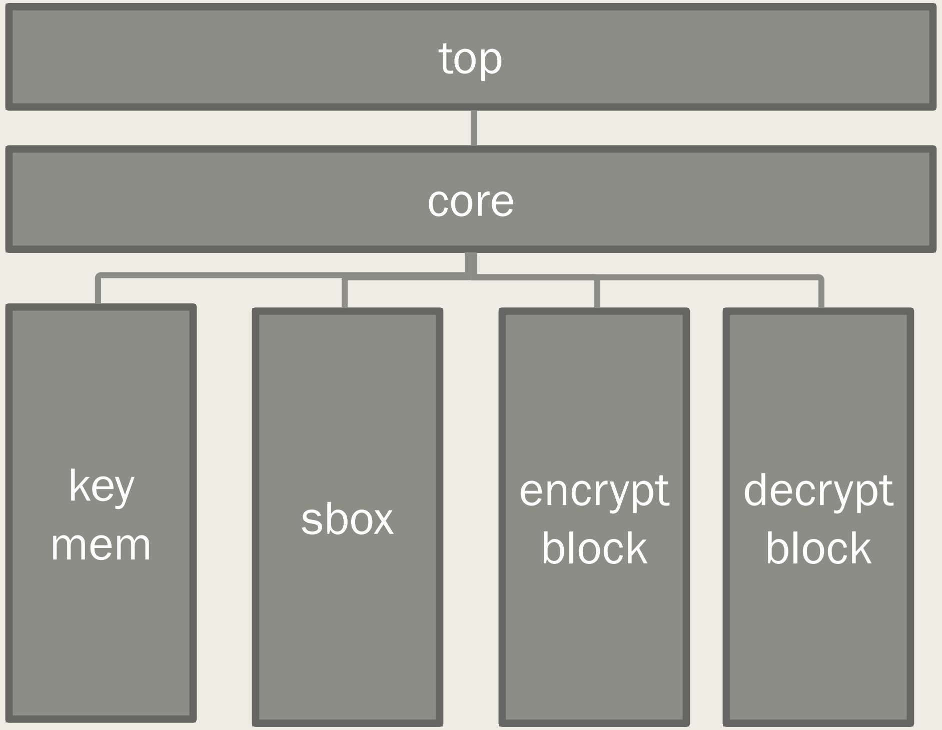
unit : cycle

AES core

- AES accelerator
- Synthesis
- Area overhead
- Software memory footprint
- Execute time comparison

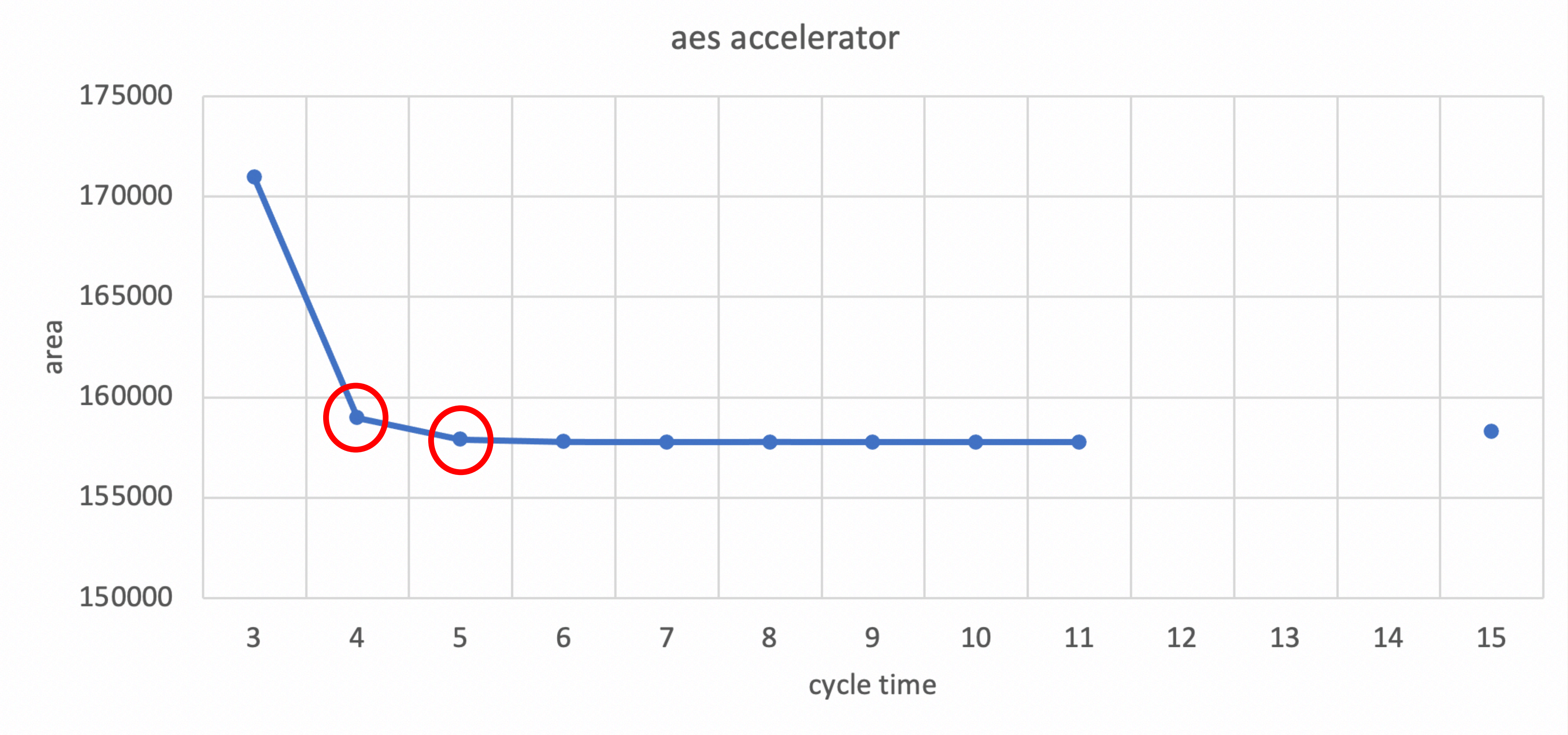
AES accelerator

- Author: Joachim Strömbergson
- Open source: https://github.com/secworks/aes (last update 2021.05)
- SecWork: Verilog Implementation of the Symmetric Block Cipher AES



Top:
Communicate with outer circuit (addr, write_data....)
Core:
Control unit, transfer roundkey to block
Key mem:
Key expansion, store roundkey
Sbox:
store look-up table
Encrypt block
Decrypt block

A-T analysis


aes accelerator
175000
170000
165000
160000
155000
150000
area
3
4
5
6
7
8
9
10
11
12
13
14
15
cycle time

Area overhead

	Base	ISE	Accelerator	Accelerator
synthesis	.13um	.13um	.13um	.13um
Cycle time	18ns	18ns	4ns	5ns
Freq	56MHz	56MHz	250MHz	200MHz
Area	189105	195176 (x1.032)	259398 (x1.37)	258308 (x1.37)
Area(-rk)	189105	195176	158985	157895

unit : um^2

Software memory footprint

	Base	ISE	Accelerator
Enc-KeyExp	148	86	0
Enc	808	290	0
Dec-KeyExp	456	64	0
Dec	1508	290	0
.data	4114	10	0

unit : byte

Execute time comparison

	Base	ISE	Accelerator
Enc-KeyExp	389 (29%)	237 (49%)	100 (42%)
Enc	955 (71%)	250 (51%)	136 (58%)
Enc total	1344	487	236 (x2.1)
Dec-KeyExp	9161 (56%)	793 (76%)	100 (42%)
Dec	7330 (44%)	251 (24%)	136 (58%)
Dec total	16491	1044	236 (x4.4)

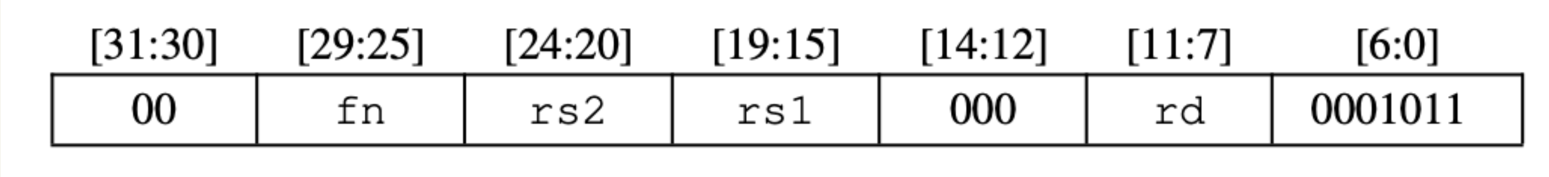
unit : cycle

AES accelerator

Speed	Base	ISE	Accelerator
Enc	x1	X2.8	X26
Dec	x1	X15.8	x312

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