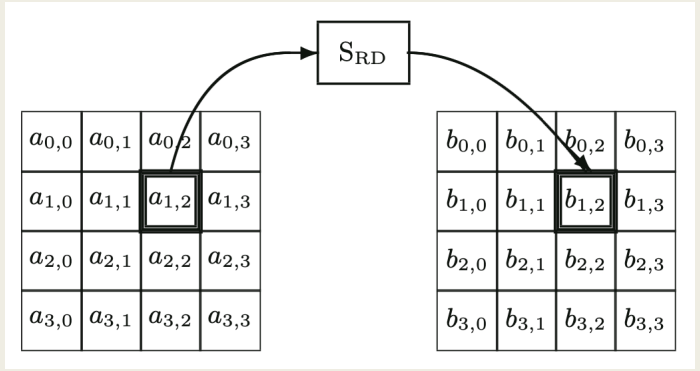
9/10 MEETING

Outline

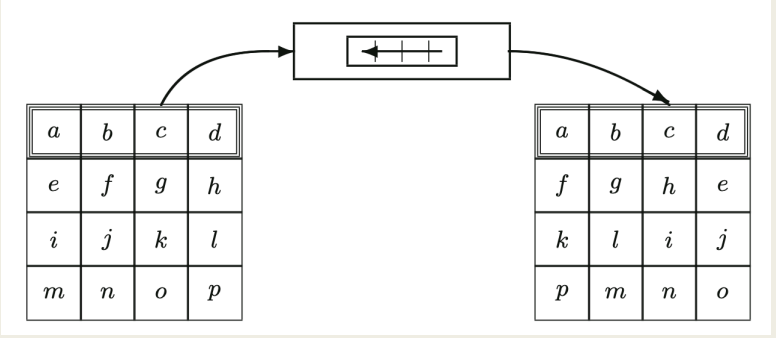
1. Calculation in AES
2. AES decryption software acceleration
3. Compare base and ISE
4. AES core (accelerator)

AES (review)

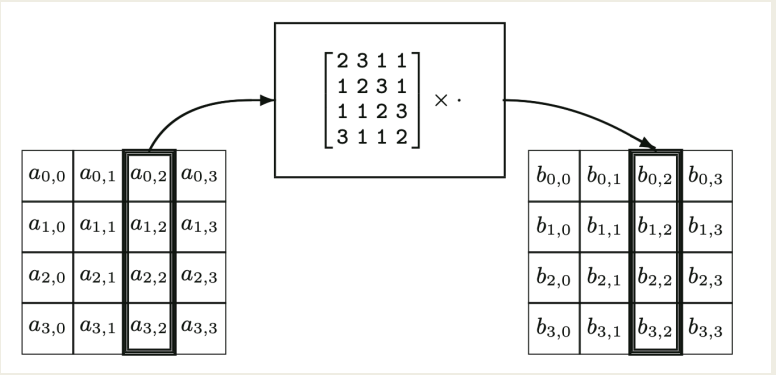
- SubBytes (S-Box)

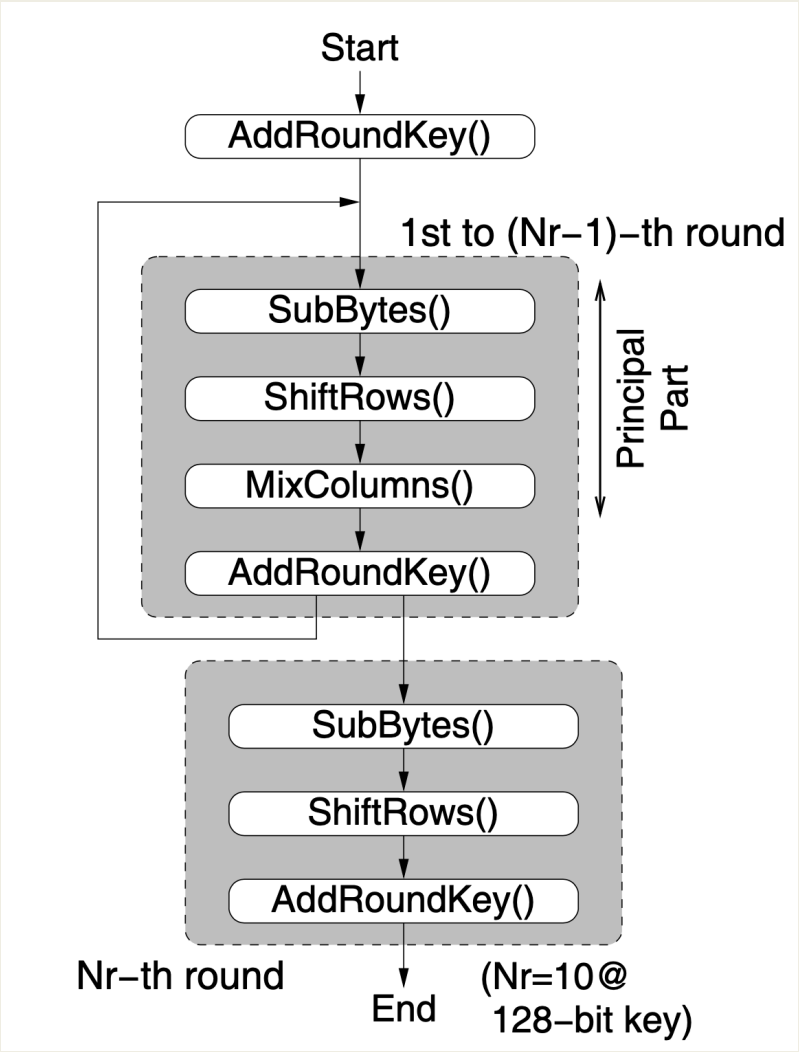


- ShiftRows



- MixColumns





Calculation in AES (review)

- 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*

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

Multiplication in AES

$$b_7b_6b_5b_4b_3b_2b_1b_0 \mapsto b(x)$$

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

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Example: (assume a_0=0x21 ,....)

$(E \times a_0) + (B \times a_1) + (D \times a_2) + (9 \times a_3)$

-> $(1110 * 00100001)$

-> $(x^3+x^2+x^1) * (x^5+1)$

-> $x^1 * (x^5+1) + x^2 * (x^5+1) + x^3 * (x^5+1)$

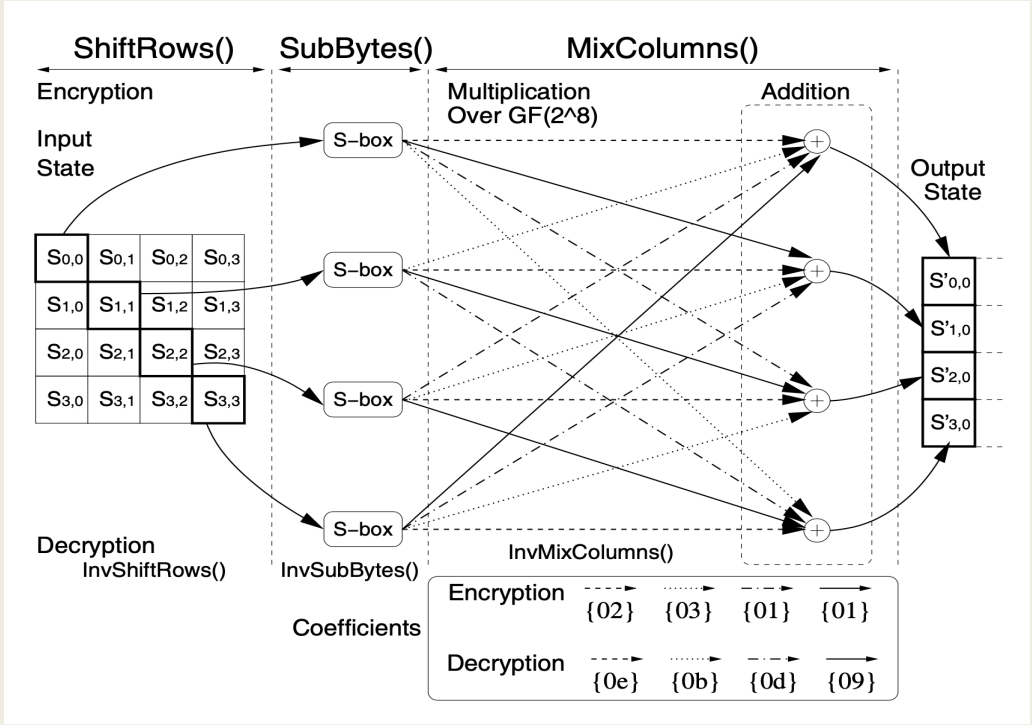
-> $(x^8 + x^7 + x^6 + x^3 + x^2 + x^1)$ *(ps. $x^8 => x^4+x^3+x^1+1$)*

-> $(x^7 + x^6 + x^4 + (1+1)x^3 + x^2 + (1+1)x^1 + 1)$

-> $(x^7 + x^6 + x^4 + x^2 + 1)$ = 11010101 = 0xD5 != 0x1CE (1 1100 1110 = 462)

AES software acceleration (for base CPU)

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



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

Software memory footprint

	Old	New	Paper
Dec-KeyExp	456	**176**	174
Dec	1508	**792**	804
Dec total	1964	**968**	978
.data	296	**4656**	5120

unit : byte

Execute time comparison

	Old	New	Paper
Dec-KeyExp	9161 (56%)	**2192 (70%)**	2307 (69%)
Dec	7330 (44%)	**951 (30%)**	1037 (31%)
Dec total	16491	**3143**	3344

unit : cycle

Analysis

- Area overhead
- Software memory footprint
- Execute time comparison

Area overhead

	Base	ISE	SCARV	SCARV-ISE
synthesis	.13um	.13um	Yosys	Yosys
Cycle time	18ns	18ns	X	X
Area	37136	38328 (x1.032)	37325	38546 (x1.033)
ISE area	0	1161 (3%)	0	1149 (3%)

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	176	64	174	64
Dec	792	290	804	290
Dec total	968	354 (-63%)	978	354 (-64%)
.data	4656	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	2192 (70%)	793 (76%)	2307 (69%)	1118 (80%)
Dec	951 (30%)	251 (24%)	1037 (31%)	286 (20%)
Dec total	3143	1044 (-67%)	3344	1404 (-58%)

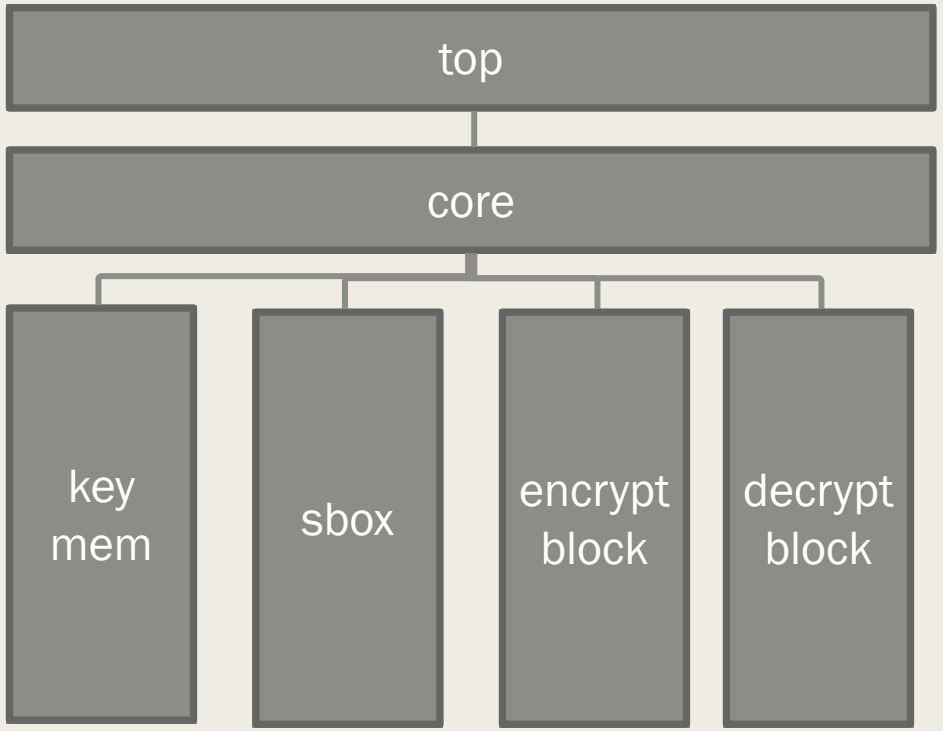
unit : cycle

AES core

- Split enc and dec in accelerator
- Area overhead
- Software memory footprint
- Execute time comparison
- Power

AES accelerator (review)

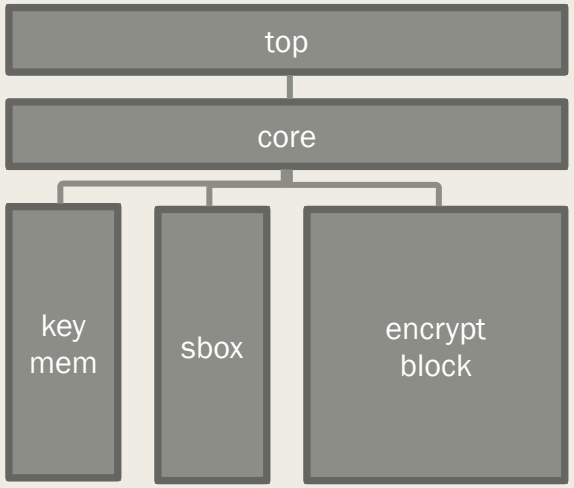
- Author: Joachim Strömbergson
- Open source: https://github.com/secworks/aes (last update 2021.05)
- SecWork: Verilog Implementation of the Symmetric Block Cipher AES

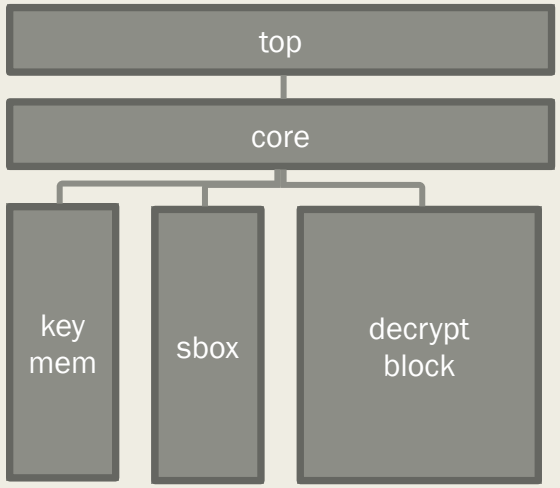


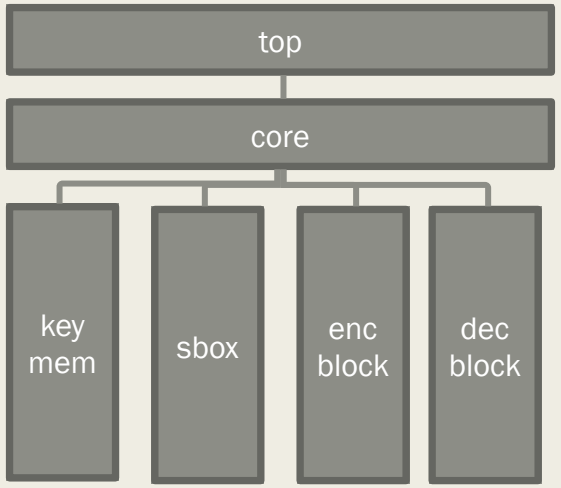
Top:
    Communicate with outer circuit (addr, write_data….)
Core:
    Control unit, transfer roundkey to block
Key mem:
    Key expansion, store roundkey
Sbox:
    store look-up table
Encrypt block
Decrypt block

Split

	Encrypt	Decrypt	Complete
Memory footprint	256 bytes	512 bytes	512 bytes
Area (-sbox-mem)	104579 um^2	112798 um^2	134782 um^2
Area	216906 um^2	236192 um^2	258176 um^2







Area overhead

	Base	ISE	Accelerator	Base+ Acc	Base+ Acc (enc)	Base+ Acc (dec)
synthesis	.13um	.13um	.13um	.13um	.13um	.13um
Cycle time	18ns	18ns	5ns	18ns	18ns	18ns
Freq	56MHz	56MHz	200MHz	56MHz	56MHz	56MHz
Area (-sbox-mem)	189105	195176	134831	323887	293684	301903
Area	189105	195176	258308	447413	406011	425297

unit : um^2

Memory footprint

	Base	ISE	Acc	Acc (enc)	Acc (dec)
Enc	956	376	0	0	0
Dec	968	354	0	0	0
.data	4656	10	512	256	512

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
Dec-KeyExp	2192 (70%)	793 (76%)	100 (42%)
Dec	951 (30%)	251 (24%)	136 (58%)
Dec total	3143	1044	236

unit : cycle

Compare

Speed	Base	ISE	Accelerator	Base + Acc
Enc	x1	x2.8	x20.4	x5.7
Dec	x1	x3.0	x47.9	x13.3

Area	Base	ISE	Accelerator	Base + Acc
Enc	x1	x1.03	x0.55	x1.55
Dec	x1	x1.03	x0.6	x1.6

Power

	Base	ISE	Acc	Acc	Acc (enc)	Acc (dec)
Cycle time	18ns	18ns	5ns	18ns	18ns	18ns
memory	17.7	17.7	0	0	0	0
internal	2.96	2.96	18.9	5.26	5.01	5.01
switching	0.5	0.49	0.106	0.03	0.028	0.028

unit : mW

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