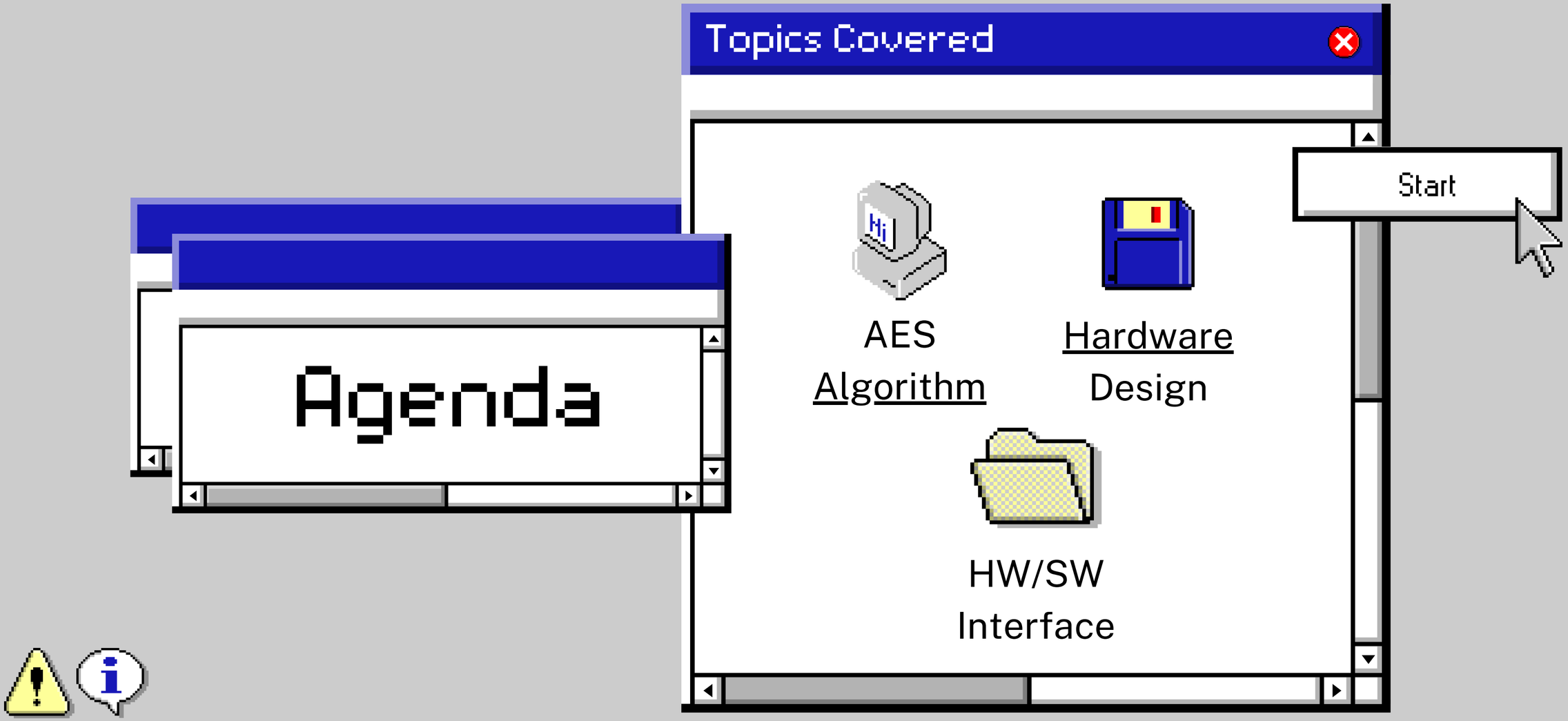
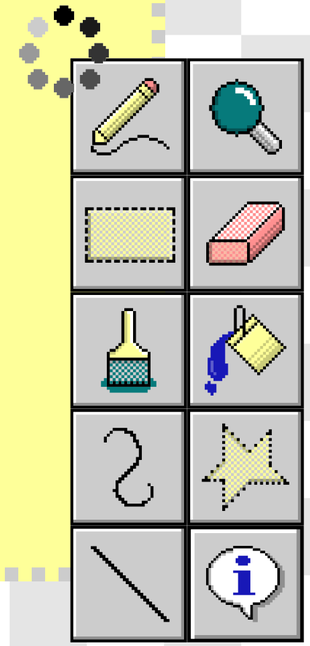
SonicSecurity: Audio Encrpytion

Tyler Chang, Jaewon Lee, Joshua Mathew

11:11PM


Topics Covered
Start
Agenda
AES
Algorithm
Hardware
Design
HW/SW
Interface

AES Algorithm

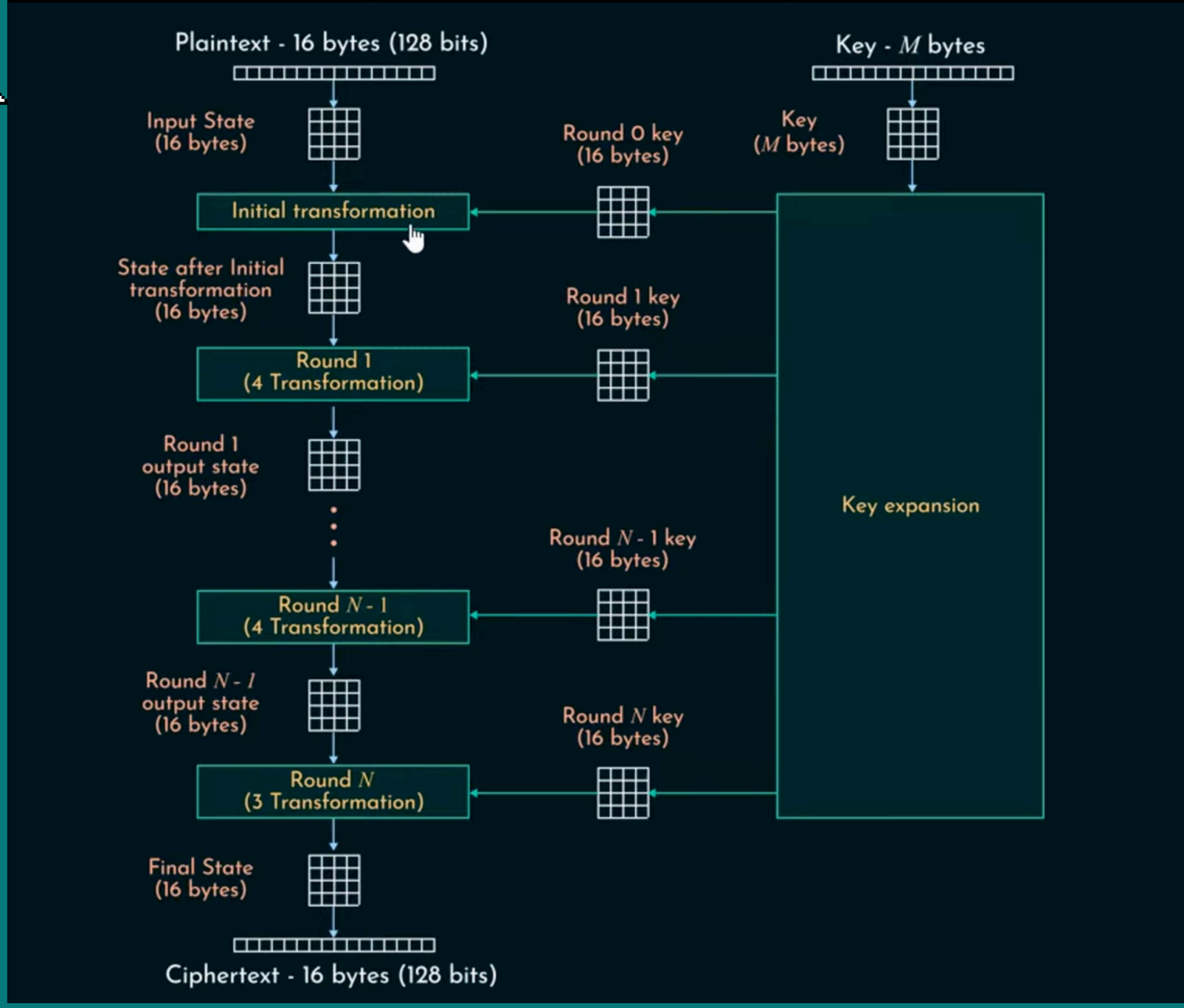


Back to Agenda Page

AES Algorithm

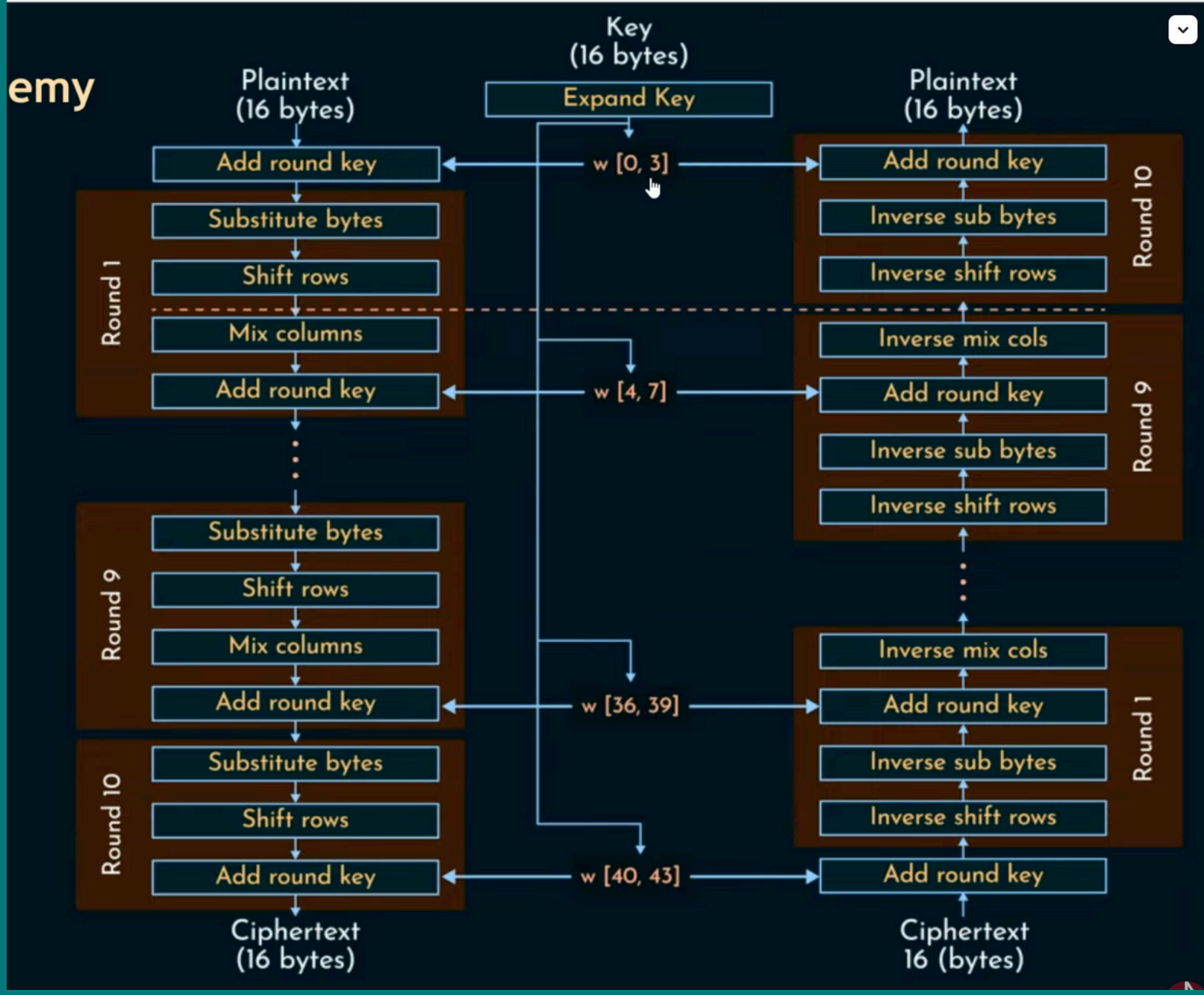
128 bit Plaintext

128 bit Key



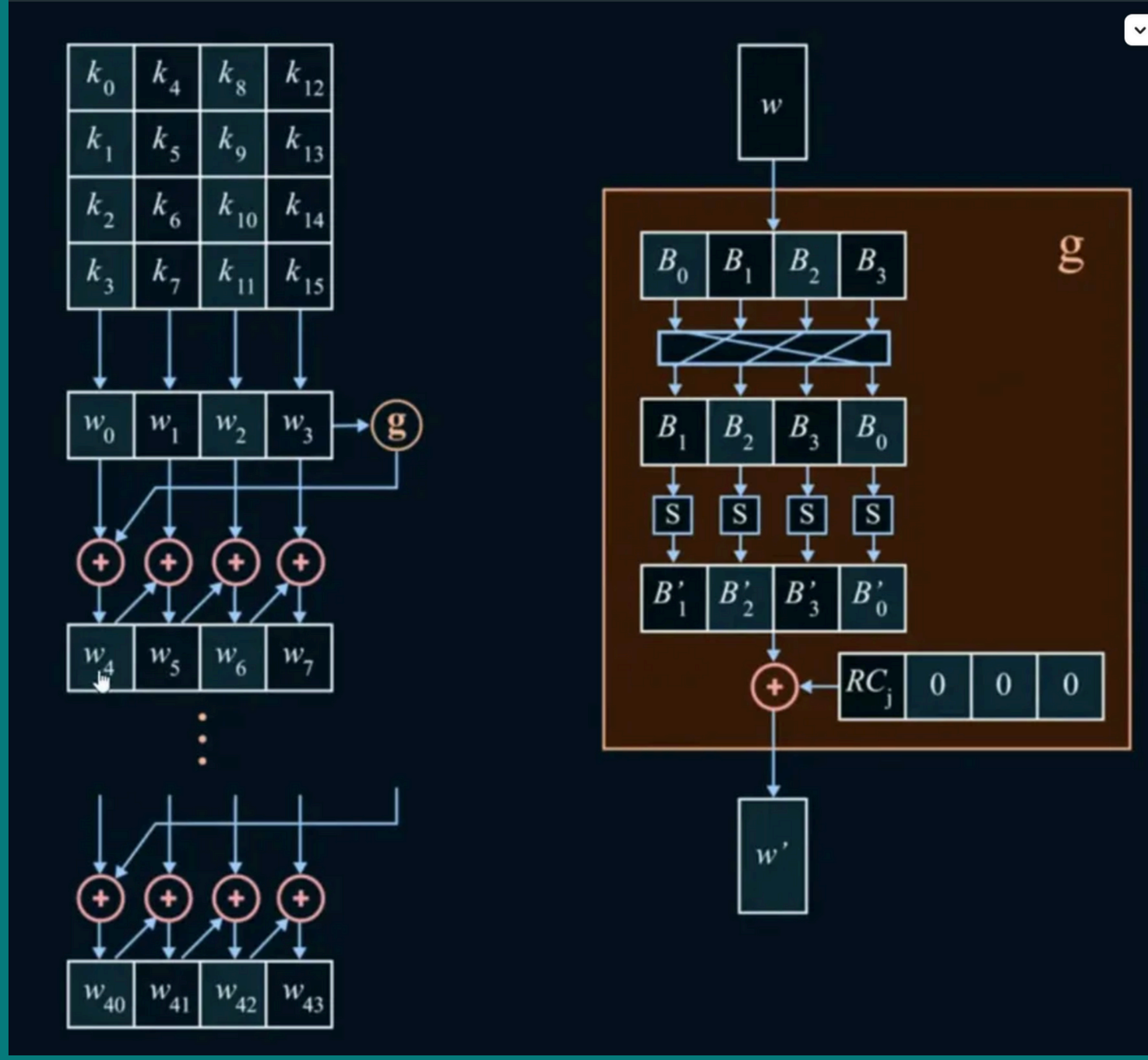
Credits: NesoAcademy

AES Encryption and Decryption Flow



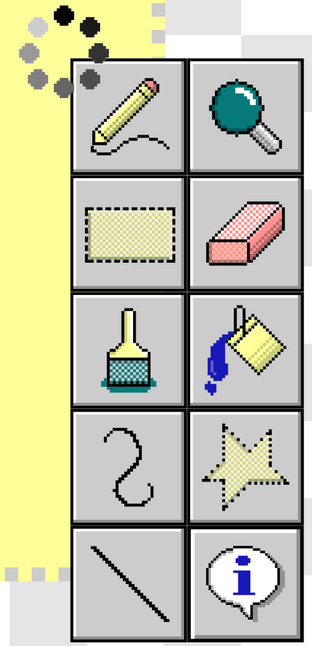
Credits: NesoAcademy

AES Key Expansion



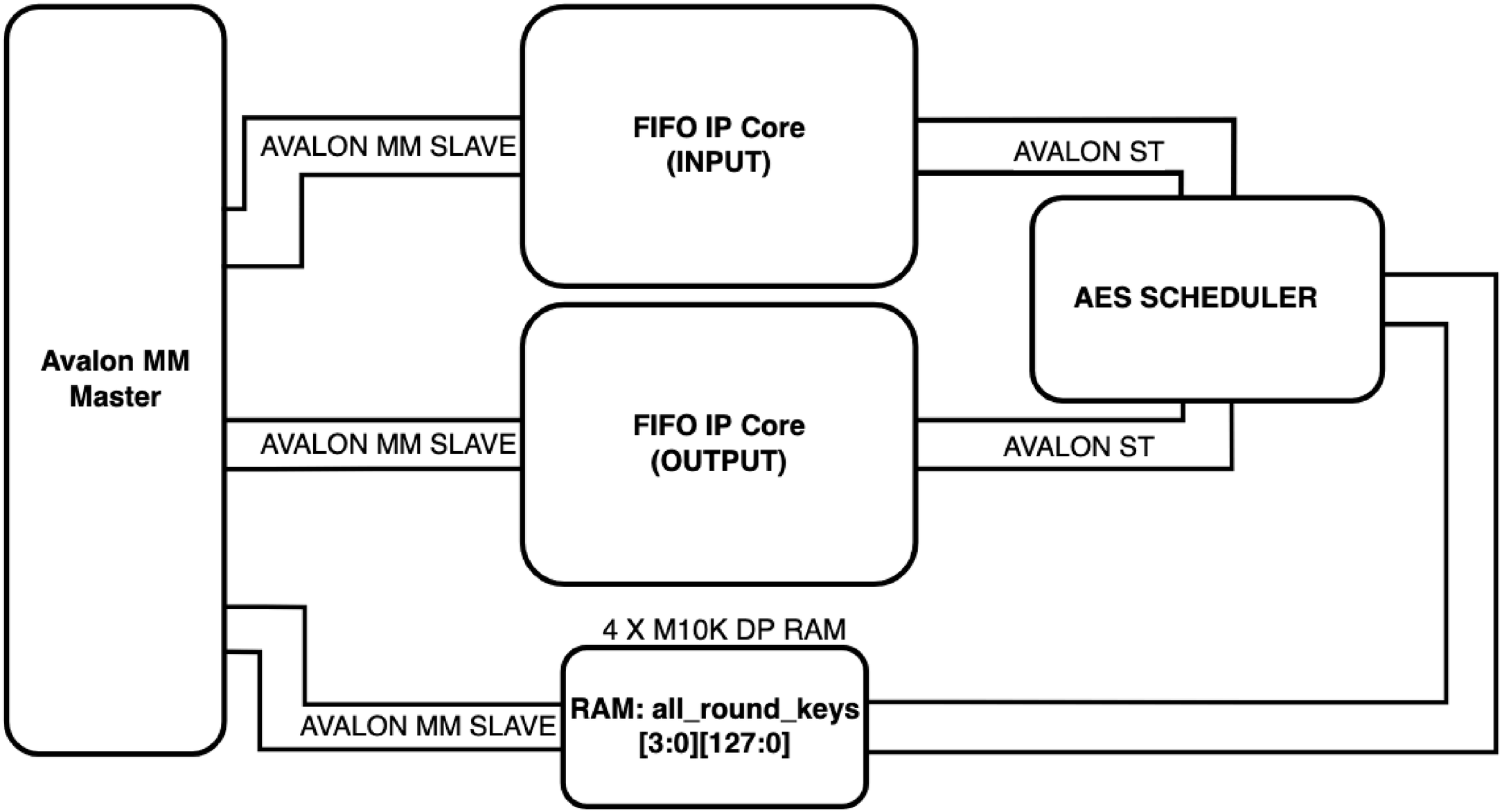
Credits: NesoAcademy

HW Design

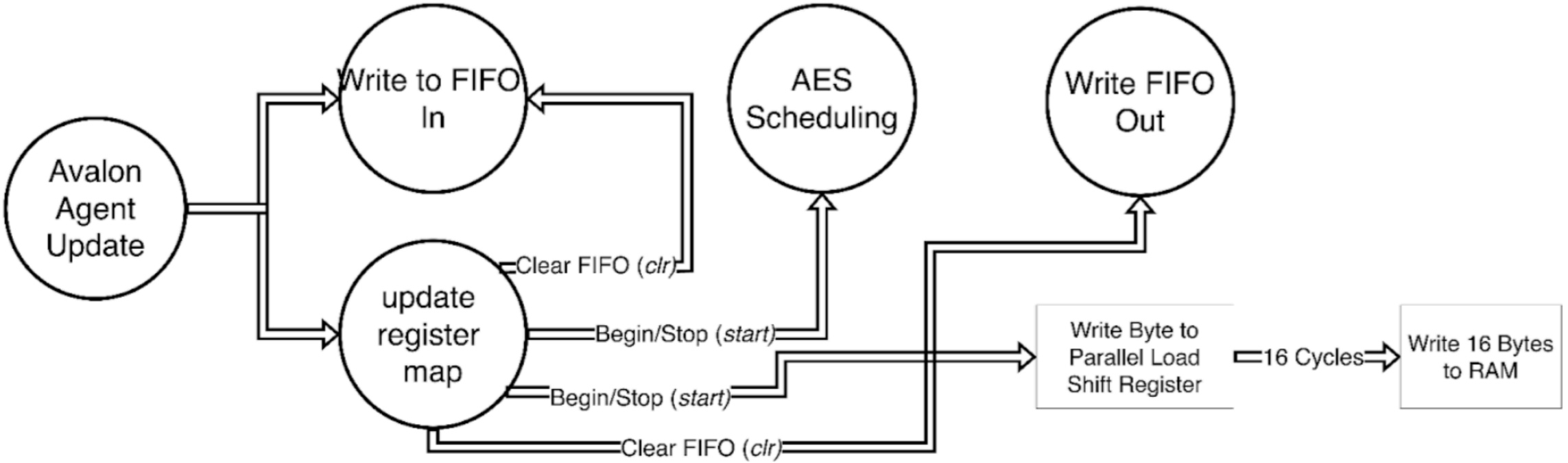


Back to Agenda Page

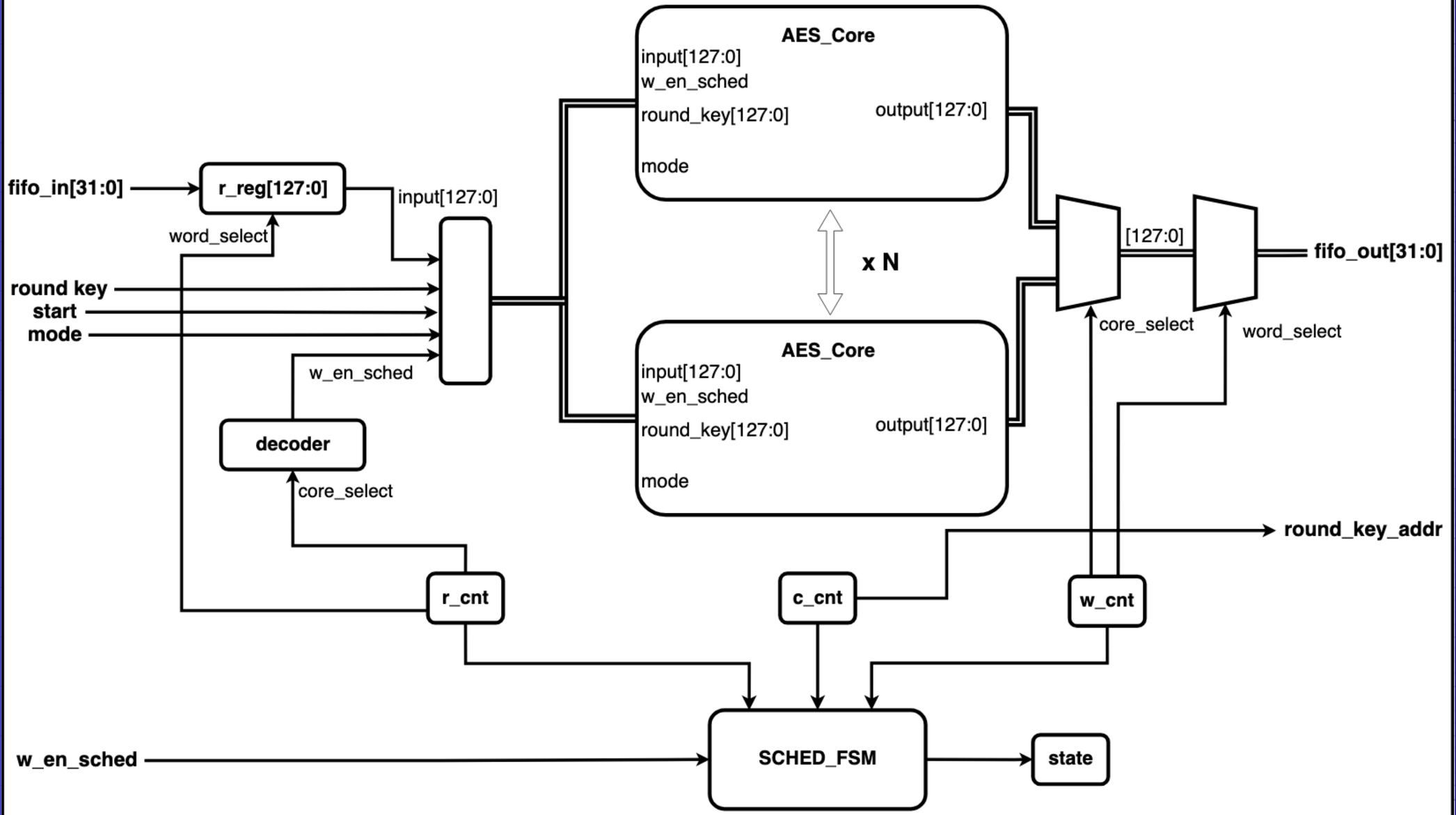
AES_TOP


Avalon MM Master
AVALON MM SLAVE
FIFO IP Core (INPUT)
AVALON ST
AES SCHEDULER
AVALON MM SLAVE
FIFO IP Core (OUTPUT)
AVALON ST
4 X M10K DP RAM
AVALON MM SLAVE
RAM: all_round_keys [3:0][127:0]

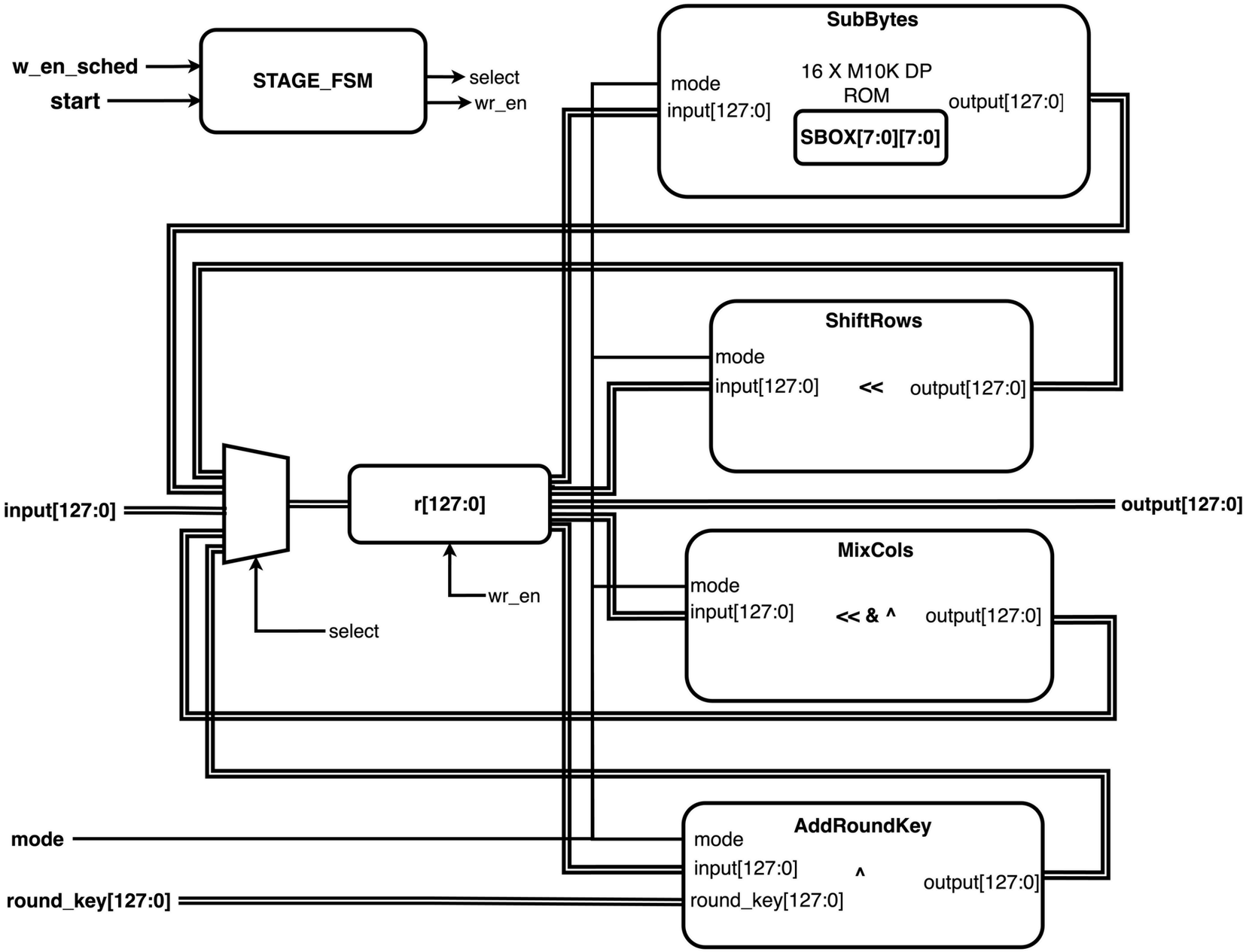
AES_TOP Control



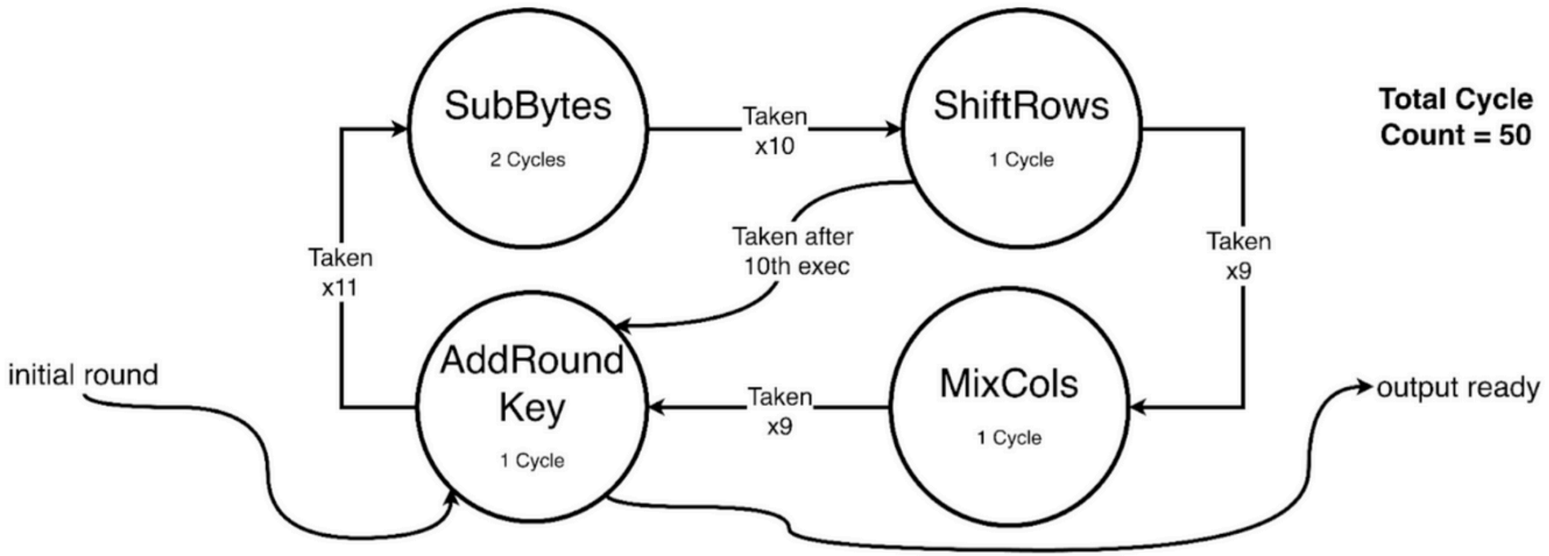
AES_SCHEDULER



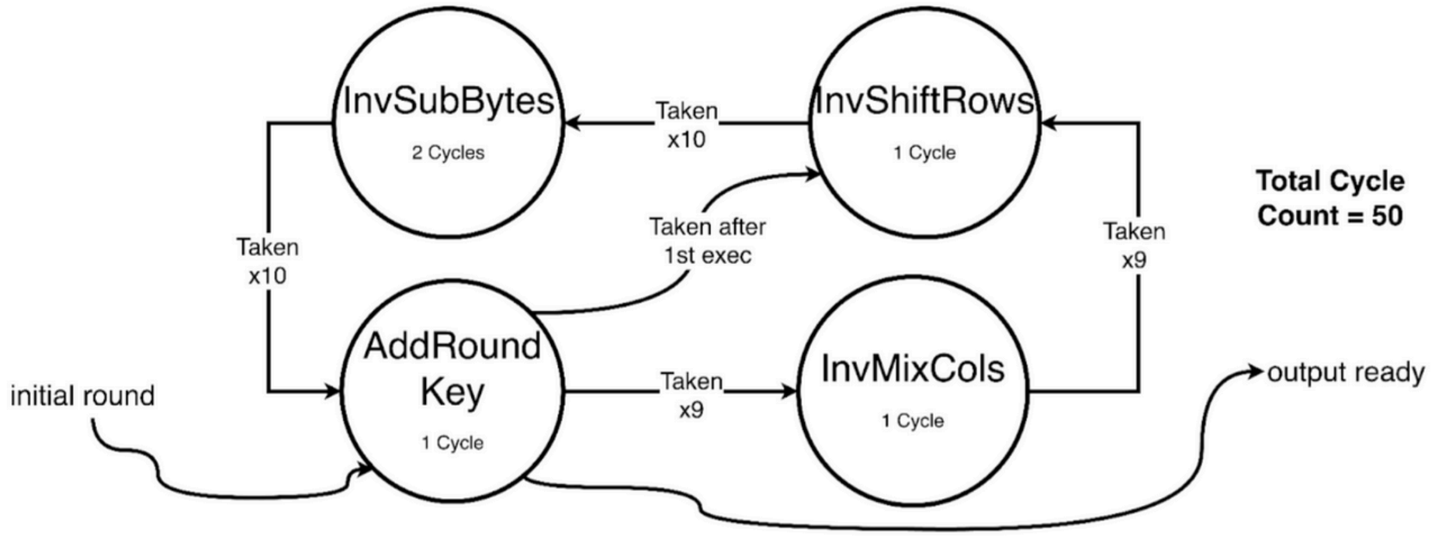
AES_CORE


w_en_sched
start
STAGE_FSM
select
wr_en
SubBytes
mode
input[127:0]
16 X M10K DP
ROM
SBOX[7:0][7:0]
output[127:0]
ShiftRows
mode
input[127:0]
<<
output[127:0]
input[127:0]
r[127:0]
output[127:0]
wr_en
select
MixCols
mode
input[127:0]
<< & ^
output[127:0]
mode
round_key[127:0]
AddRoundKey
mode
input[127:0]
^
round_key[127:0]
output[127:0]

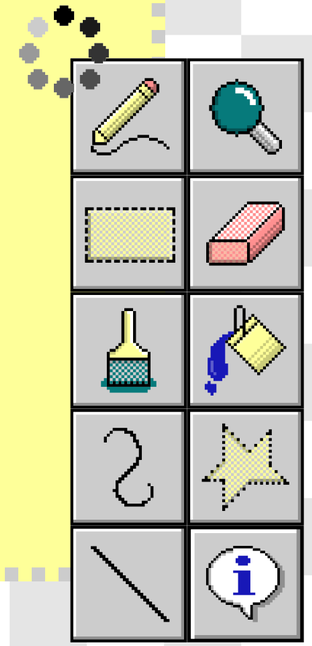
AES Encryption Control Flow



AES Decryption Control Flow



HW/SW Interface



Back to Agenda Page

Register Map

BYTE ADDR	REGISTER MAP	
0x00 - 0xff	round_key_ram [31:0]	W
0x100 - 0x11f	out_csr [1:0]	R
0x120 - 0x13f	in_csr [1:0]	R
0x140 - 0x147	out_data [31:0]	R
0x148 - 0x14f	in_data [31:0]	W
0x150 -0x153	ctl [1:0]	R/W

RAM and CTL Register

- Avlon MM Master 32bit Lightweight
  - 256B Dual Port Mixed width RAM
  - 4B Control register

Dual Port
Mixed
Width RAM
32b-128b

ctl							
31						1	0
						mode	start

MM to ST FIFO Interface

FIFO MM Interface

in_data/out_data							
7	6	5	4	3	2	1	0
x	x	x	x	DATA3	DATA2	DATA1	DATA0

FIFO Status Register

offset	31					24	23					16	15					8	7	6	5	4	3	2	1	0
base	fill_level																									
base + 1																					i_status				
base + 2																					event				
base + 3																					interrupt enable				
base + 4	almostfull																									
base + 5	almostempty																									

Kernel Drivers

- Writing to input FIFO
- Reading from output FIFO
- Writing round keys to RAM
- Writing control (mode and start)

User Space Program

- WAV File Processing
- Key Expansion Algorithm

Benchmarks

Python Comparison

```
❯ python3 aes_ecb.py encrypt piano-20sec.wav out.wav 2B7E151628AED2A6ABF7158809C
F4F3C
File encrypted successfully: out.wav
Encryption time: 44.0441 seconds
Total processing time (including I/O): 44.0462 seconds
File size: 3850.89 KB
Encryption speed: 87.43 KB/s
❯ python3 aes_ecb.py decrypt out.wav out2.wav 2B7E151628AED2A6ABF7158809CF4F3C
File decrypted successfully: out2.wav
Decryption time: 85.1089 seconds
Total processing time (including I/O): 85.1104 seconds
File size: 3850.89 KB
Decryption speed: 45.25 KB/s
```

```
❯ python3 aes_ecb.py encrypt seven-nation-army.wav out.wav 2B7E151628AED2A6ABF71
58809CF4F3C
File encrypted successfully: out.wav
Encryption time: 485.9267 seconds
Total processing time (including I/O): 485.9396 seconds
File size: 41064.00 KB
Encryption speed: 84.51 KB/s
❯ python3 aes_ecb.py decrypt out.wav out2.wav 2B7E151628AED2A6ABF7158809CF4F3C
File decrypted successfully: out2.wav
Decryption time: 918.4220 seconds
Total processing time (including I/O): 918.4337 seconds
File size: 41064.00 KB
Decryption speed: 44.71 KB/s
```

Appendix B — Cipher Example

The following diagram shows the values in the state array as the cipher progresses for a block length and a key length of 16 bytes each (i.e., $Nb = 4$ and $Nk = 4$).

```
Input  = 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34
Key    = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
```

The Round Key values are taken from the Key Expansion example in Appendix A.1.

Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns	Round Key Value
input	32 88 31 e0 43 5a 31 37 f6 30 98 07 a8 8d a2 34				2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c
1	19 a0 9a e9 3d f4 c6 f8 e3 e2 8d 48 be 2b 2a 08	d4 e0 b8 1e 27 bf b4 41 11 98 5d 52 ae f1 e5 30	d4 e0 b8 1e bf b4 41 27 5d 52 11 98 30 ae f1 e5	04 e0 48 28 66 cb f8 06 81 19 d3 26 e5 9a 7a 4c	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05
2	a4 68 6b 02 9c 9f 5b 6a 7f 35 ea 50 f2 2b 43 49	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	49 45 7f 77 db 39 02 de 87 53 d2 96 3b 89 f1 1a	58 1b db 1b 4d 4b e7 6b ca 5a ca b0 f1 ac a8 e5	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f
3	aa 61 82 68 8f dd d2 32 5f e3 4a 46 03 ef d2 9a	ac ef 13 45 73 c1 b5 23 cf 11 d6 5a 7b df b5 b8	ac ef 13 45 c1 b5 23 73 d6 5a cf 11 b8 7b df b5	75 20 53 bb ec 0b c0 25 09 63 cf d0 93 33 7c dc	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b
4	48 67 4d d6 6c 1d e3 5f 4e 9d b1 58 ee 0d 38 e7	52 85 e3 f6 50 a4 11 cf 2f 5e c8 6a 28 d7 07 94	52 85 e3 f6 a4 11 cf 50 c8 6a 2f 5e 94 28 d7 07	0f 60 6f 5e d6 31 c0 b3 da 38 10 13 a9 bf 6b 01	ef a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00
5	e0 c8 d9 85 92 63 b1 b8 7f 63 35 be e8 c0 50 01	e1 e8 35 97 4f fb c8 6c d2 fb 96 ae 9b ba 53 7c	e1 e8 35 97 fb c8 6c 4f 96 ae d2 fb 7c 9b ba 53	25 bd b6 4c d1 11 3a 4c a9 d1 33 c0 ad 68 8e b0	d4 7c ca 11 d1 83 f2 f9 c6 f8
6	f1 c1 7c 5d 00 92 c8 b5 6f 4c 8b d5 55 ef 32 0c	a1 78 10 4c 63 4f e8 d5 a8 29 3d 03 fc df 23 fe	a1 78 10 4c 4f e8 d5 63 3d 03 a8 29 fe fc df 23	4b 2c 33 37 86 4a 9d d2 8d 89 f4 18 6d 80 e8 d8	6d 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd
7	26 3d e8 fd 0e 41 64 d2 2e b7 72 8b 17 7d a9 25	f7 27 9b 54 ab 83 43 b5 31 a9 40 3d f0 ff d3 3f	f7 27 9b 54 83 43 b5 ab 40 3d 31 a9 3f f0 ff d3	14 46 27 34 15 16 46 2a b5 15 56 d8 bf ec d7 43	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f
8	5a 19 a3 7a 41 49 e0 8c 42 dc 19 04 b1 1f 65 0c	be d4 0a da 83 3b e1 64 2c 86 d4 f2 c8 c0 4d fe	be d4 0a da 3b e1 64 83 d4 f2 2c 86 fe c8 c0 4d	00 b1 54 fa 51 c8 76 1b 2f 89 6d 99 d1 ff cd ea	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f
9	ea 04 65 85 83 45 5d 96 5c 33 98 b0 f0 2d ad c5	87 f2 4d 97 ec 6e 4c 90 4a c3 46 e7 8c d8 95 a6	87 f2 4d 97 6e 4c 90 ec 46 e7 4a c3 a6 8c d8 95	47 40 a3 4c 37 d4 70 9f 94 e4 3a 42 ed a5 a6 bc	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e
10	eb 59 8b 1b 40 2e a1 c3 f2 38 13 42 1e 84 e7 d2	e9 cb 3d af 09 31 32 2e 89 07 7d 2c 72 5f 94 b5	e9 cb 3d af 31 32 2e 09 7d 2c 89 07 b5 72 5f 94		d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6
output	39 02 dc 19 25 dc 11 6a 84 09 85 0b 1d fb 97 32				