CECS 378: Intro to Computer Security Principles

Lecture 4

Louis Uuh

Week 5

Advance Encryption Standard (AES)

- Published by NIST in November 2001
- Based on a competition won by Rijmen and Daemen (Rijndael) from Belgium
- 22 submissions, 7 did not satisfy all requirements 15 submissions 5 finalists: Mars, RC6, Rijndael, Serpent,Twofish. Winner: Rijndael.
- AES restricts it to:
  - ➢Block Size: 128 bits
  - ➢Key sizes: 128, 192, 256 (AES-128, AES-192, AES-256)

Advance Encryption Standard (AES)

- Similar to DES algorithm, in which the plaintext is process in blocks
  - Block size → 128 bit plaintext
  - # of rounds → 10 rounds
  - Master Key size → 128 bits
  - # of sub-keys → 44 sub-keys
  - Each round uses 4 keys
  - Pre-Round Calculation → 4 sub-keys
  - Cipher text → 128 bits

AES Block Diagram

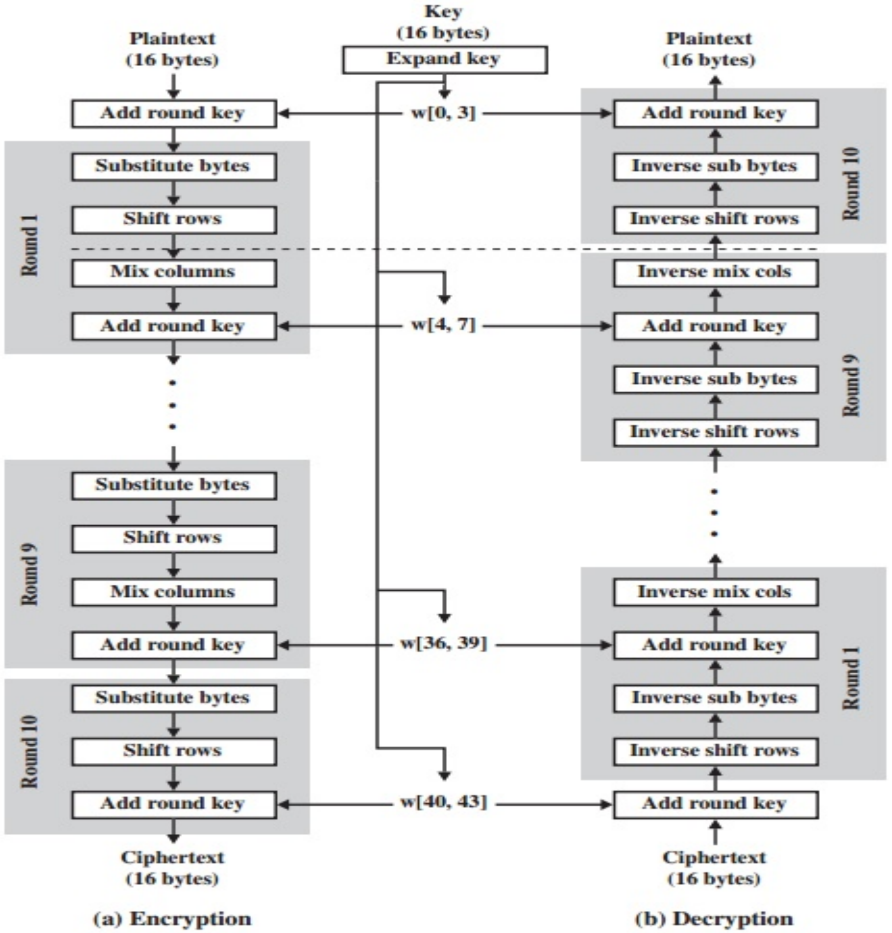


Figure 5.3 AES Encryption and Decryption

AES Input Representation

- Input to the encryption is a single 128-bit block
- Block is depicted as a 4X4 square matrix of bytes

In$_0$	In$_4$	In$_8$	In$_{12}$
In$_1$	In$_5$	In$_9$	In$_{13}$
In$_2$	In$_6$	In$_{10}$	In$_{14}$
In$_3$	In$_7$	In$_{11}$	In$_{15}$

State Array

BEACH

- Also know as Intermediate result array
- After the final stage, State is copied to an output matrix

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Output Array

- Also represented as a 4X4 table
- Each square represents one byte or 8 bits just like the previous ones

Out_0	Out_4	Out_8	Out_{12}
Out_1	Out_5	Out_9	Out_{13}
Out_2	Out_6	Out_{10}	Out_{14}
Out_3	Out_7	Out_{11}	Out_{15}

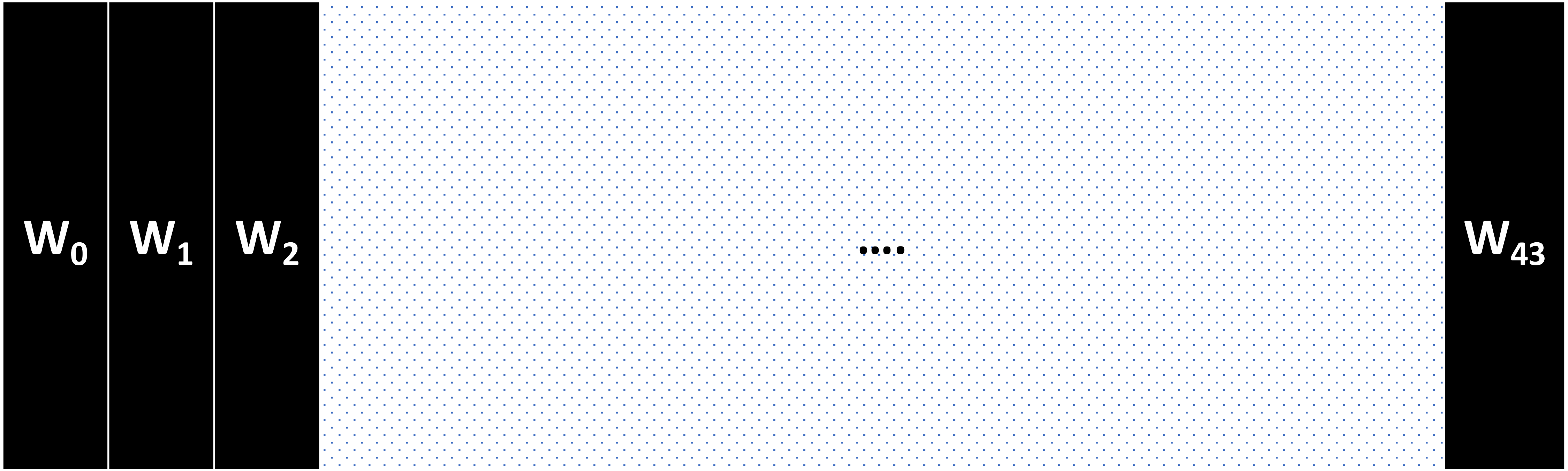
Key Array

- Similarly the key is store as a 4x4 table
- 128-bits or 4 words

K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

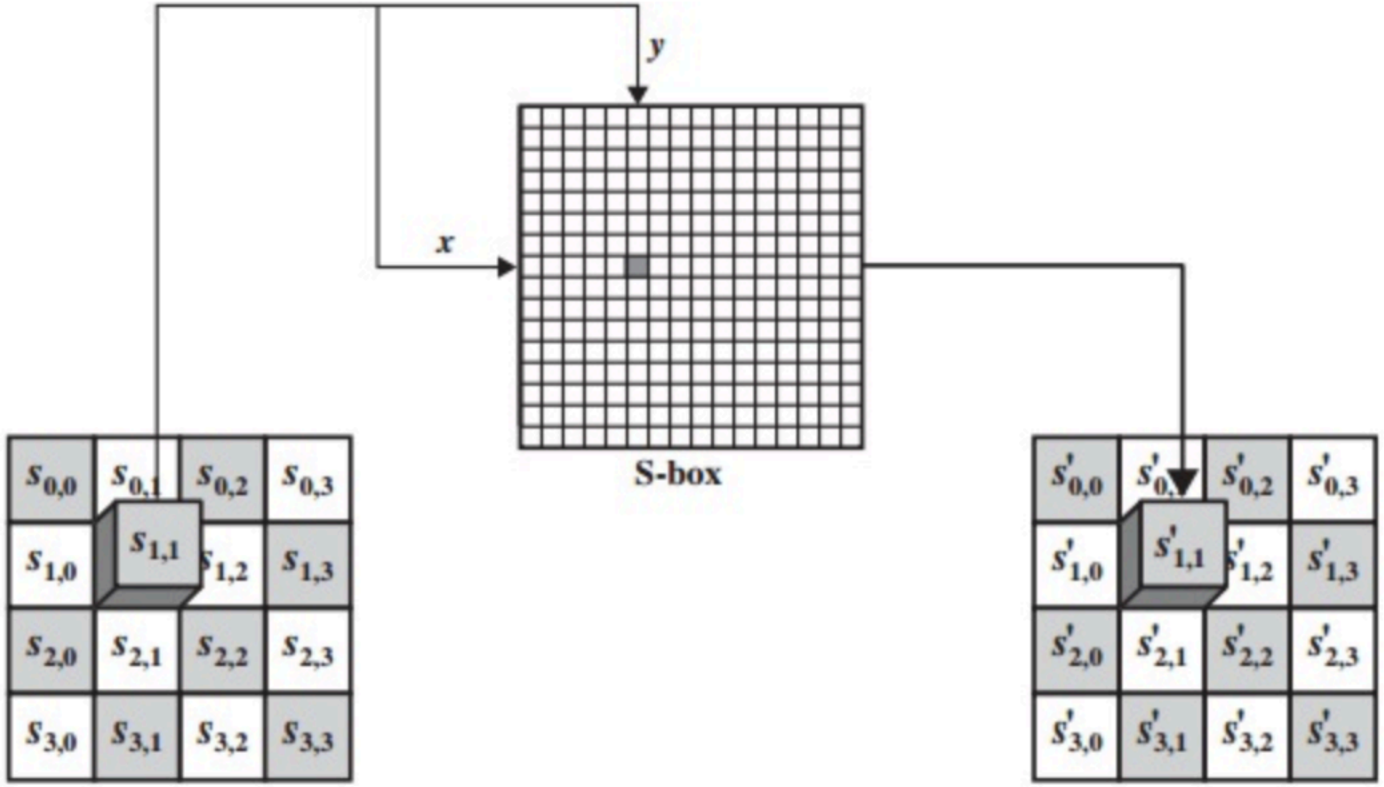
Key Expansion

- 44 words → from W_0 to W_{43}
- Where 40 words are use in 10 rounds & 4 words in pre-initialization



Substitution Bytes

- Also called SubBytes
- It is nothing but a simple look-up table
- Contains a permutation of all possible 256 8-bit values
- Leftmost 4 bits of the byt e are used as a row
- Rightmost 4 bits are used as a column value



$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

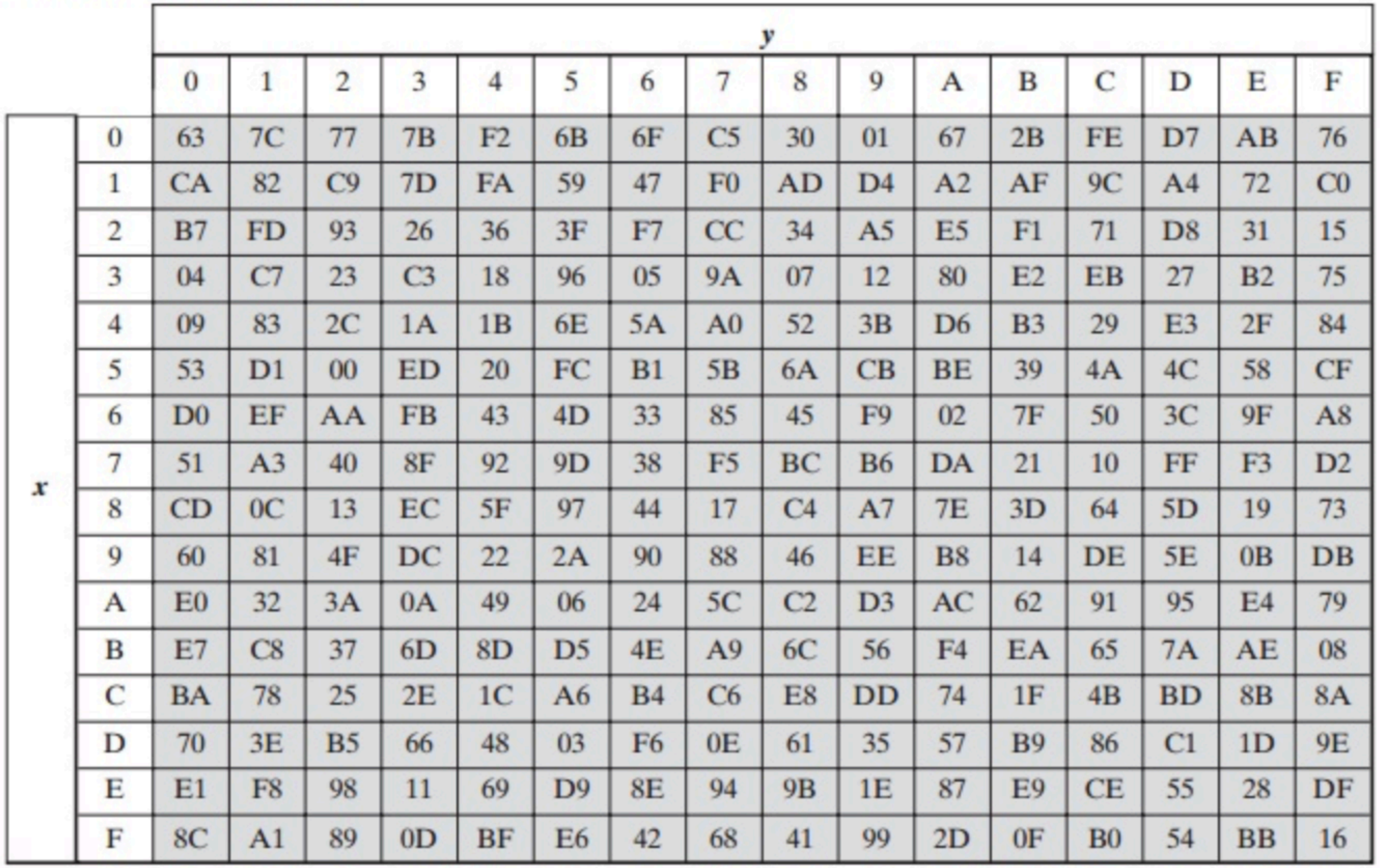
$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$

(a) Substitute byte transformation

S-Box

- Consider the following example:
- 0100 1011
- Row = 4
- Colum = B
- Result is 4B = B3
- Which then converted into bits 1011 0011

Table 5.2 AES S-Boxes

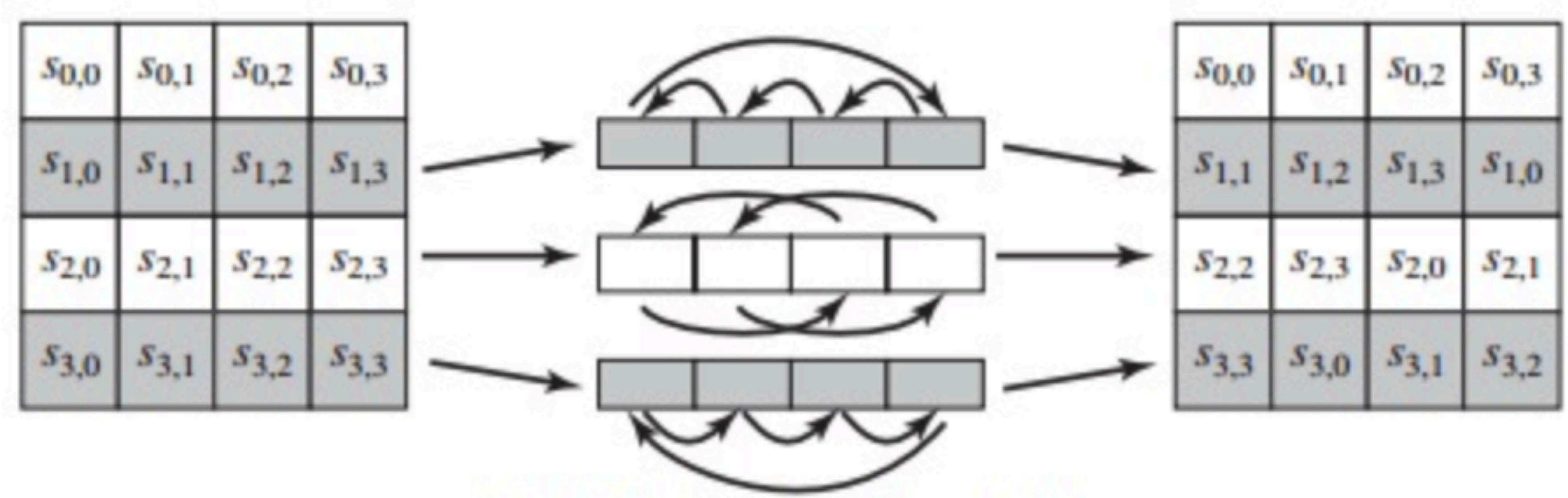


		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(a) S-box

Shift Rows

- Row 0 → 0 bits, circular right shift
- Row 1 → 1 bit, circular right shift
- Row 2 → 2 bits Row 3 → 3 bits



$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

(a) Shift row transformation

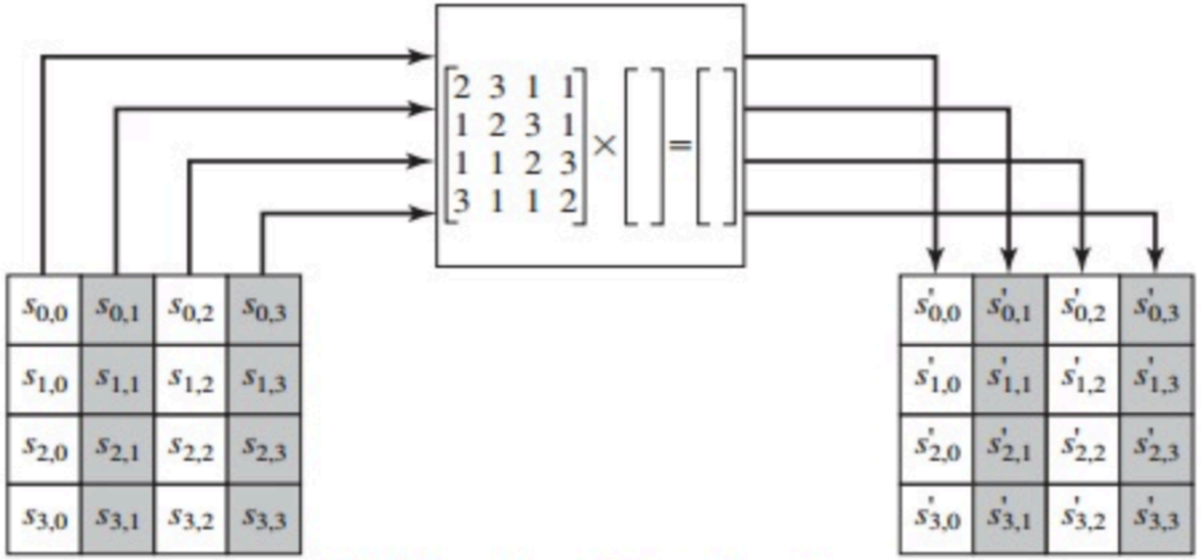
State’ Array

- Input from S-Box would be store in State Array
- This is only for S-Box and is the input for Shift Rows

$S`_{0,0}$	$S`_{0,1}$	$S`_{0,2}$	$S`_{0,3}$
$S`_{1,0}$	$S`_{1,1}$	$S`_{1,2}$	$S`_{1,3}$
$S`_{2,0}$	$S`_{2,1}$	$S`_{2,2}$	$S`_{2,3}$
$S`_{3,0}$	$S`_{3,1}$	$S`_{3,2}$	$S`_{3,3}$

Mix Columns

- Output from Shift rows would be consider input for Mix Column
- Consider each column as one word
- Take one word and apply the multiplication operation



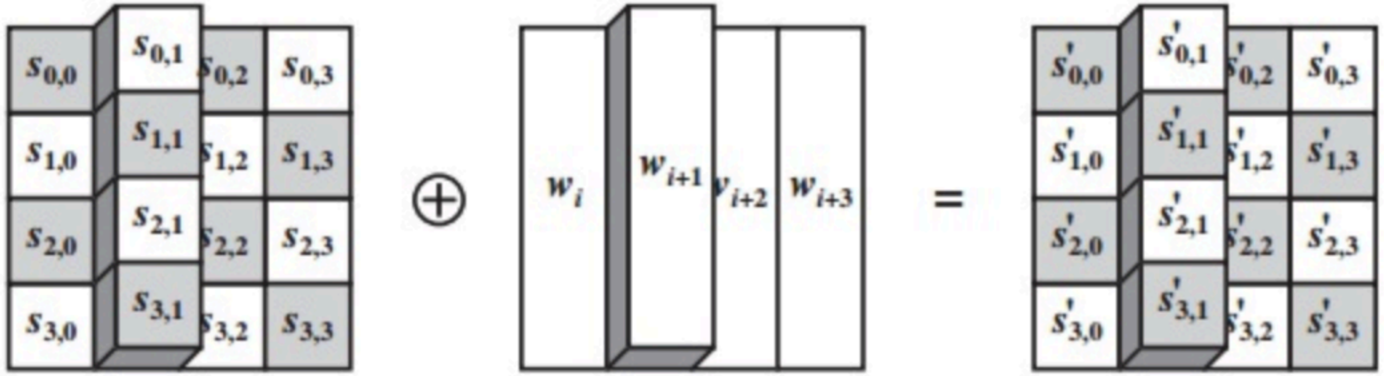
$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} \\ \\ \\ \end{bmatrix} = \begin{bmatrix} \\ \\ \\ \end{bmatrix}$
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

(b) Mix column transformation

Figure 5.7 AES Row and Column Operations

AddRound Key Transformation

- Here we are adding 4 keys, and adding here means XOR operation
- Consider 1st column one word & XOR with 1st word of Key
- Consider 2nd column as the second word & XOR with 2nd word of Key



(b) Add round key transformation

Figure 5.5 AES Byte-Level Operations

News Articles

BEΛCH

- **DDoS attack disrupts online forum used by Hong Kong protestors**
- The main forum used by Hong Kong protestors to strategize and organize rallies called LIHKG was recently hit by a DDoS attack on August 31.The site operators, who work anonymously, have stated that part of the attacks originated from websites in China (such as Baidu, the largest search engine in China and Qihoo360, a Chinese internet security firm) and there is substantial reasoning to believe that a world power was behind the attacks due to the amount of resources used. - Catherine Pham