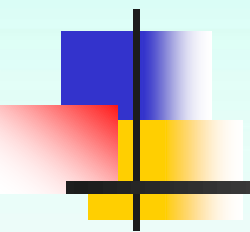


CRYPTOGRAPHY

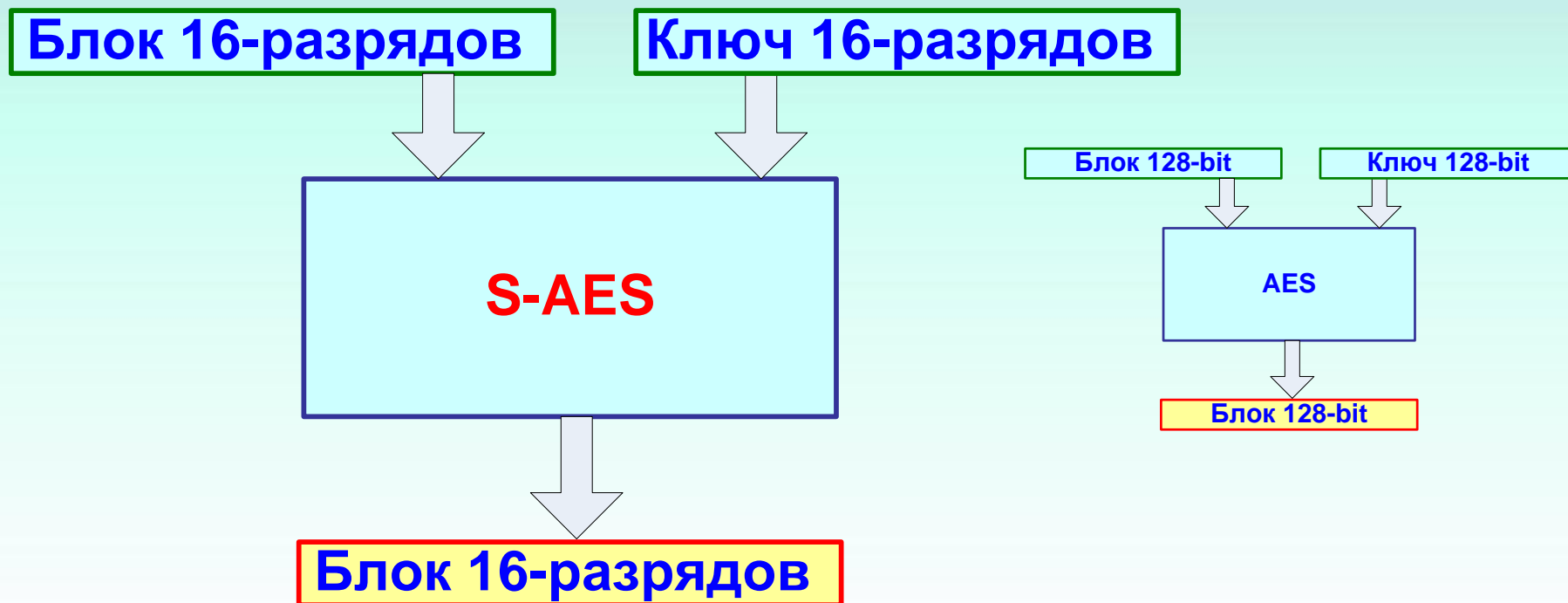


МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ШИФР S-AES

МОДЕЛИРОВАНИЕ AES

СТРУКТУРА S-AES



N_r - число раундов = 2
 $i \in \{0, 1, 2\}$

S-AES

Бит (bit)
Полубайт (nibble)
Слово (word)
Блок (block)
Состояние (state)

Одна цифра Hex

Полубайт

b_0 b_1 b_2 b_3

Слово (w)

n_0 n_1

n_0
 n_1

2 байта

Блок ()

n_0 n_1 n_2 n_3

4 nibble

S

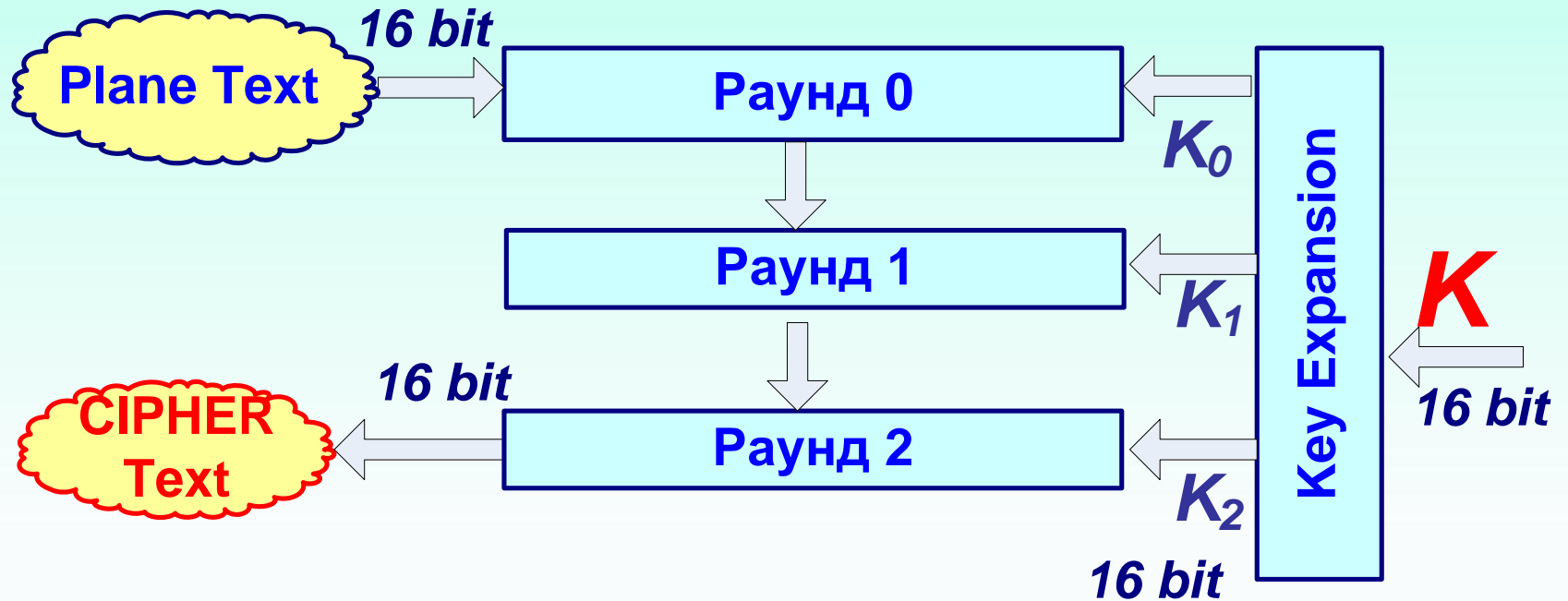
$S_{0,0}$

$S_{0,1}$

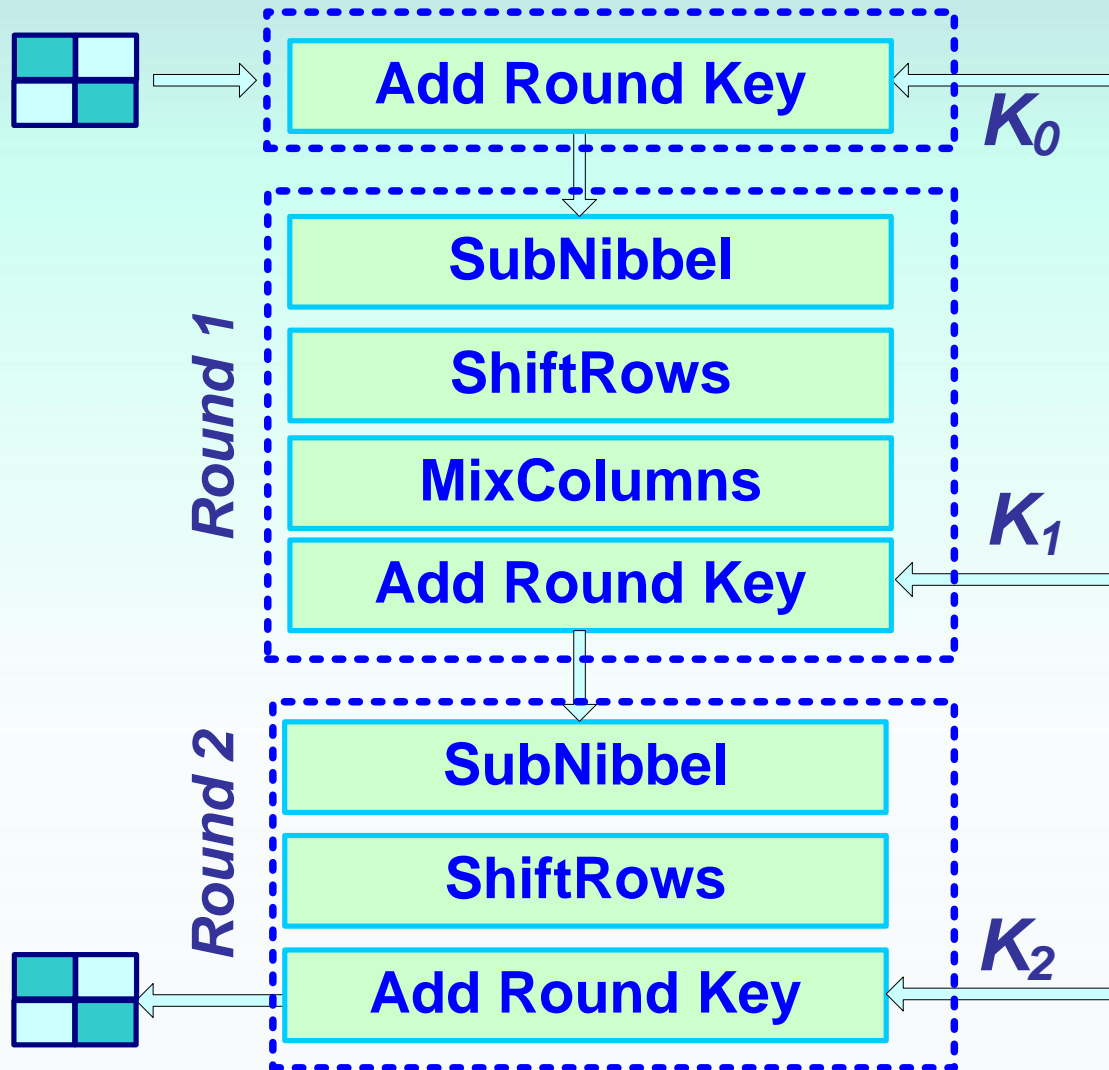
$S_{1,0}$

$S_{1,1}$

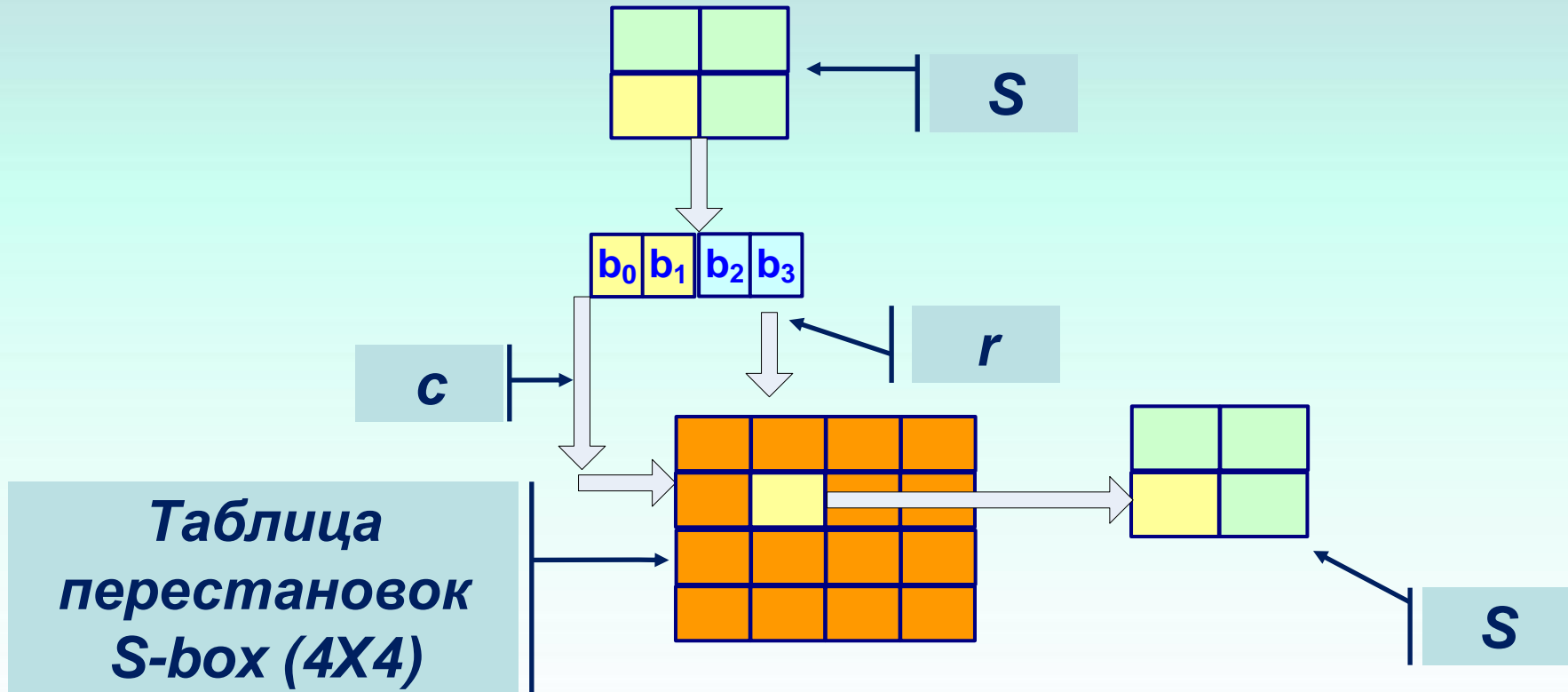
S-AES



S-AES



S-AES SubNibbles



9	4	A	B
D	1	8	5
6	2	0	3
C	E	F	7

Direct

Invers

A	5	9	B
1	7	8	F
6	0	2	3
C	4	D	E

Прямая и инверсная таблицы SubNibbles

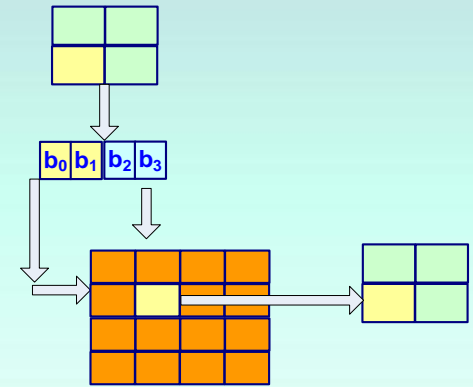
S-AES SubNibbles

3	A
5	7

3 = 00 11₂ 11₂ = 3

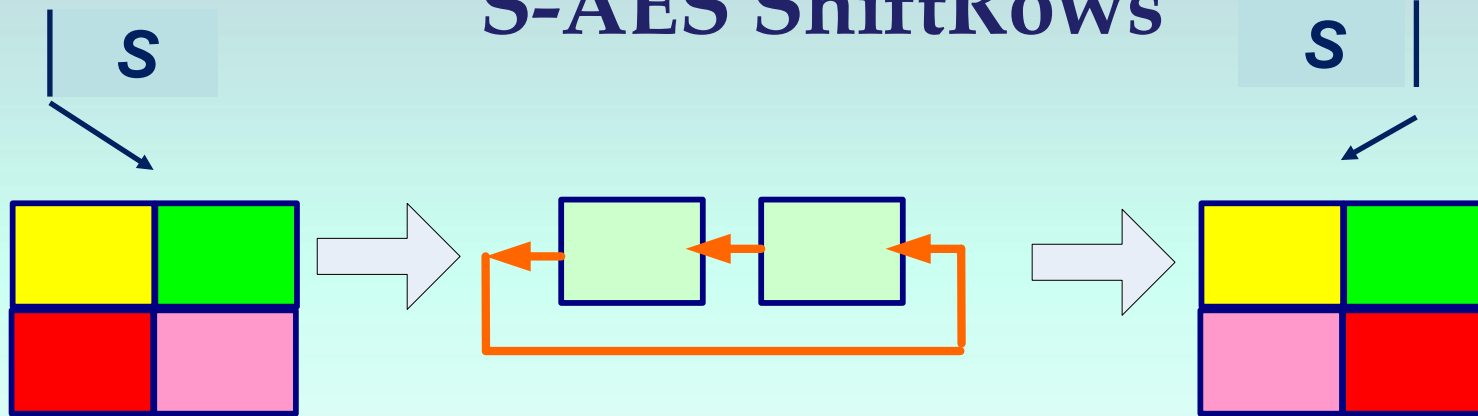
00₂ = 0

9	4	A	B
D	1	8	5
6	2	0	3
C	E	F	7



B	

S-AES ShiftRows



Первая строка : нет сдвига

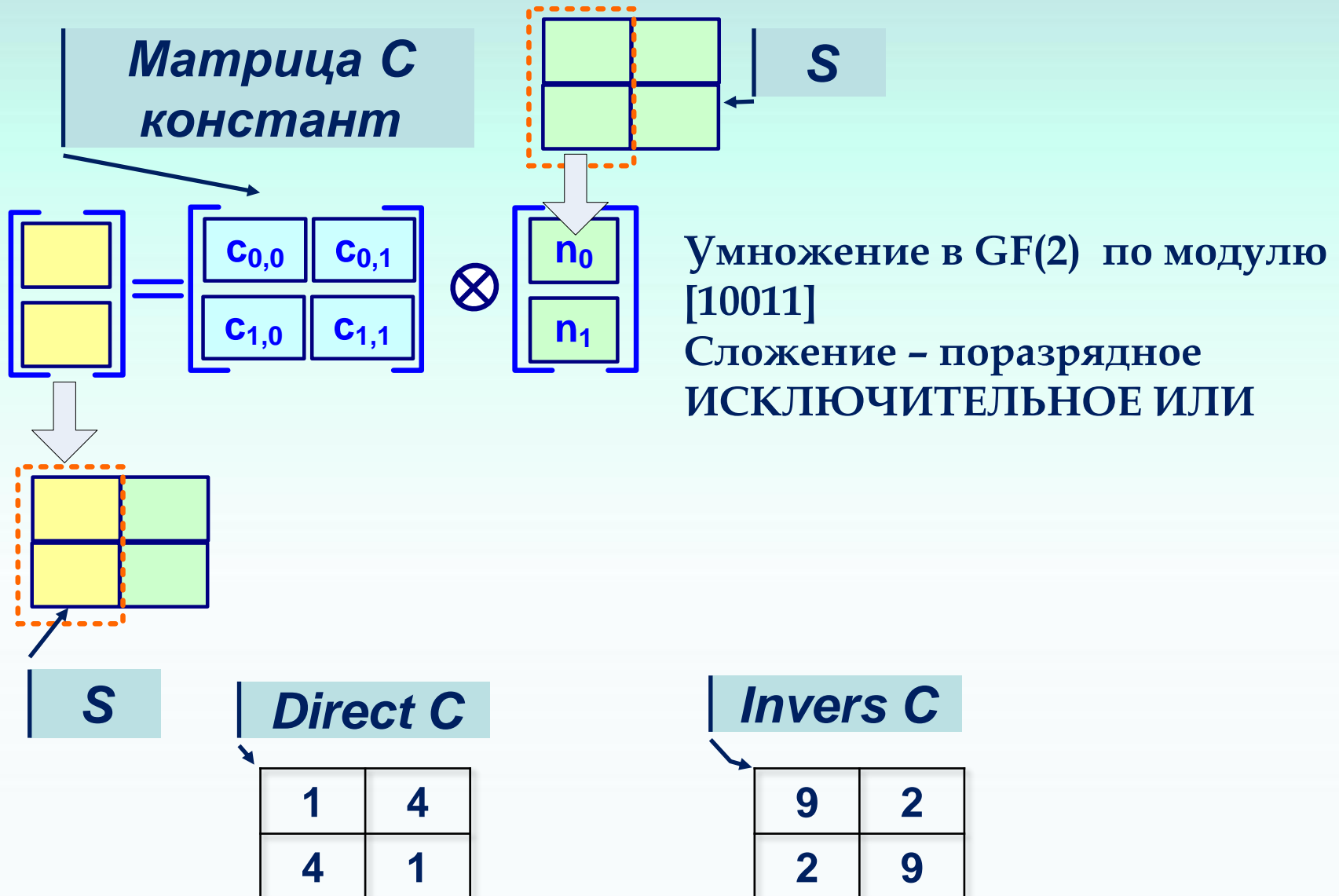
**Первая строка : сдвиг на 1 полубайт
(полубайты меняются местами)**

3	A
5	7



3	A
7	5

S-AES MixColumns

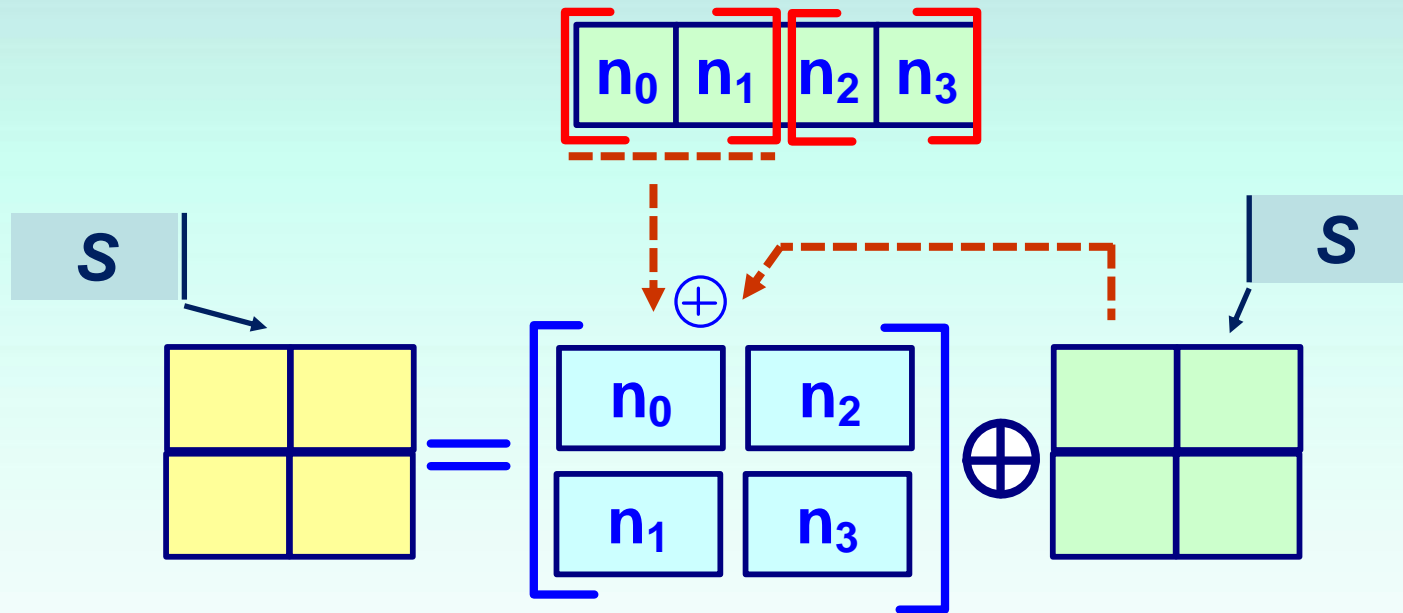


S-AES MixColumns

$$\begin{aligned}\text{StateOUT}[0][0] = & \\ & \text{CONST}[0][0] \odot \text{StateIN}[0][0] \oplus \\ & \text{CONST}[0][1] \odot \text{StateIN}[1][0]\end{aligned}$$

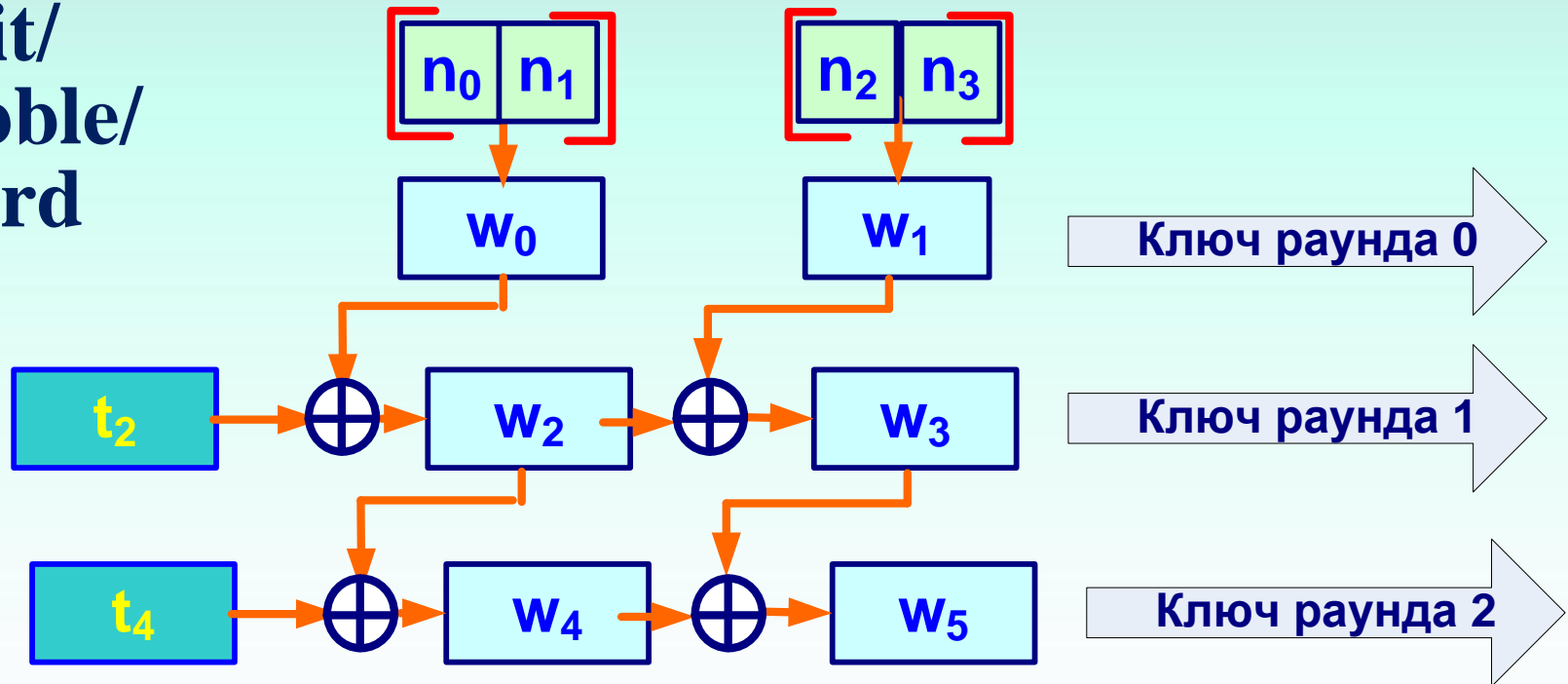
$$\begin{aligned}\text{StateOUT}[0][0] \\ = \text{StateIN}[0][0] \oplus (4 \odot \text{StateIN}[1][0]) \bmod [10011]\end{aligned}$$

S-AES AddRoundKey

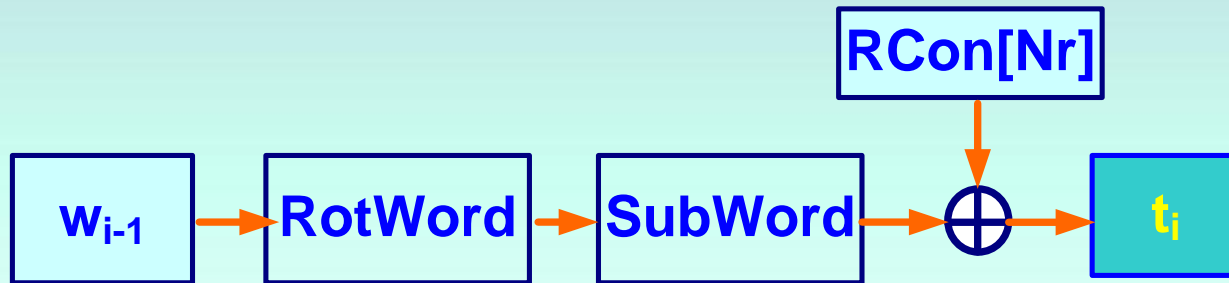


S-AES KeyExpansion

Ключ шифра
16 bit/
4 nibble/
2 word



S-AES KeyExpansion



RotWord – аналог **ShiftRow** , но применяется только к одной строке. Циклический сдвиг влево на один полубайт (меняет местами).

RCon[1]=80Hex
RCon[2]=30Hex

SubWord – аналог **SubByte** , но применяется только к одной строке. Принимает байт в слове и заменяет его другим (используя прямую таблицу **SubNibbles**).

16-ричные ЦИФРЫ

HEX	Nibble
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111

HEX	Nibble
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

S-AES Задание 1

Самостоятельно написать
InvSubNibbles

Самостоятельно ShiftRows и
InvShiftRows

Самостоятельно KeyExpansion