Simplified AES

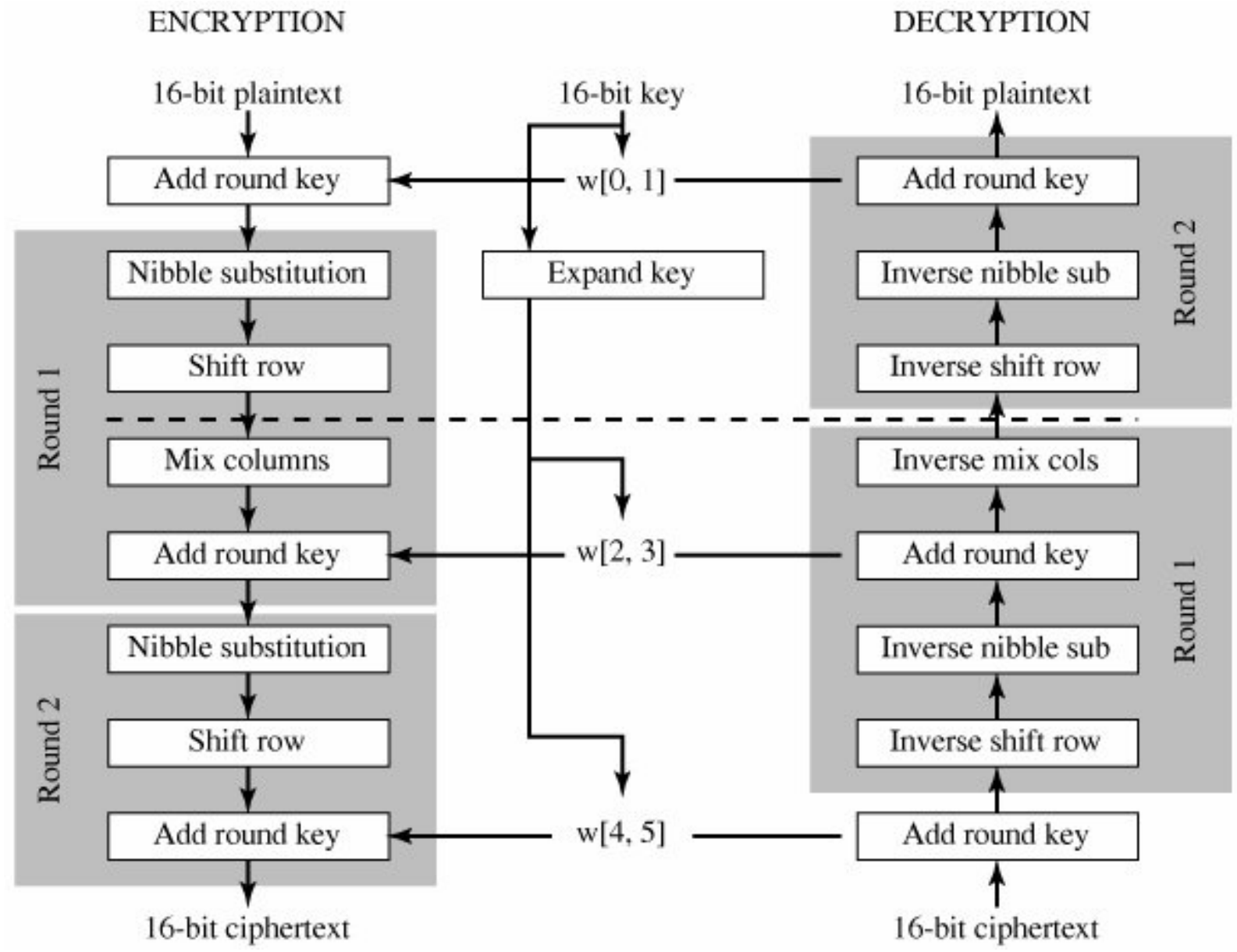
Simplified AES

- Simplified AES Structure
- Uses Modular Polynomial Arithmetic GF(2^4)

$$m(x) = x^4 + x + 1$$

- Plaintext Block Size 16 Bit (2 Bytes)
- Variable Key Size 16 Bit (2 Bytes)
- Number of Rounds 1 Round
- Round Key Size 16 Bit (2 Bytes)

Simplified AES Structure



Simplified AES Structure

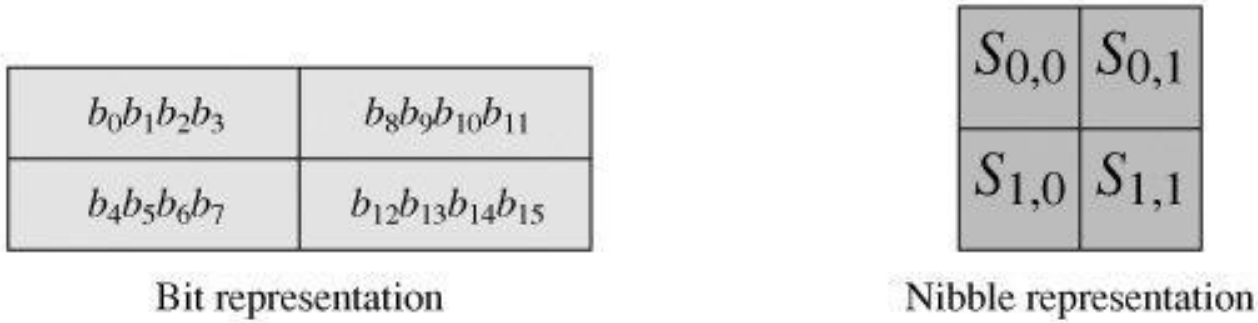
$$S-AES\ \ Encryption$$

$$A_{k_2} \circ SR \circ NS \circ A_{k_1} \circ MC \circ SR \circ NS \circ A_{k_0}$$

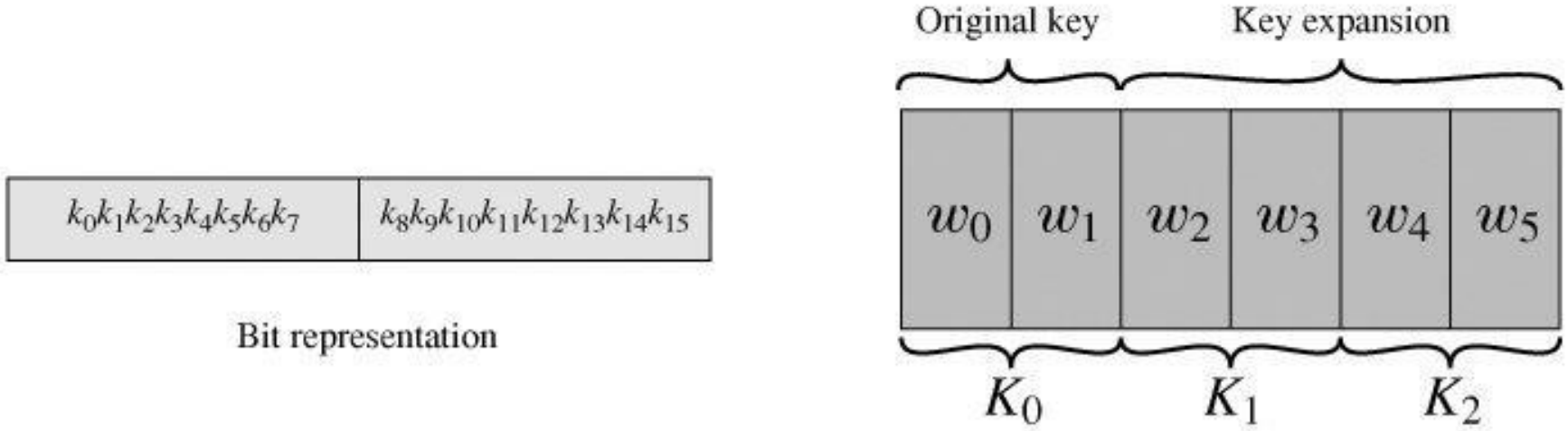
$$S-AES\ \ Decryption$$

$$A_{k_0} \circ INS \circ ISR \circ IMC \circ A_{k_1} \circ INS \circ ISR \circ A_{k_2}$$

Simplified AES Date Representation

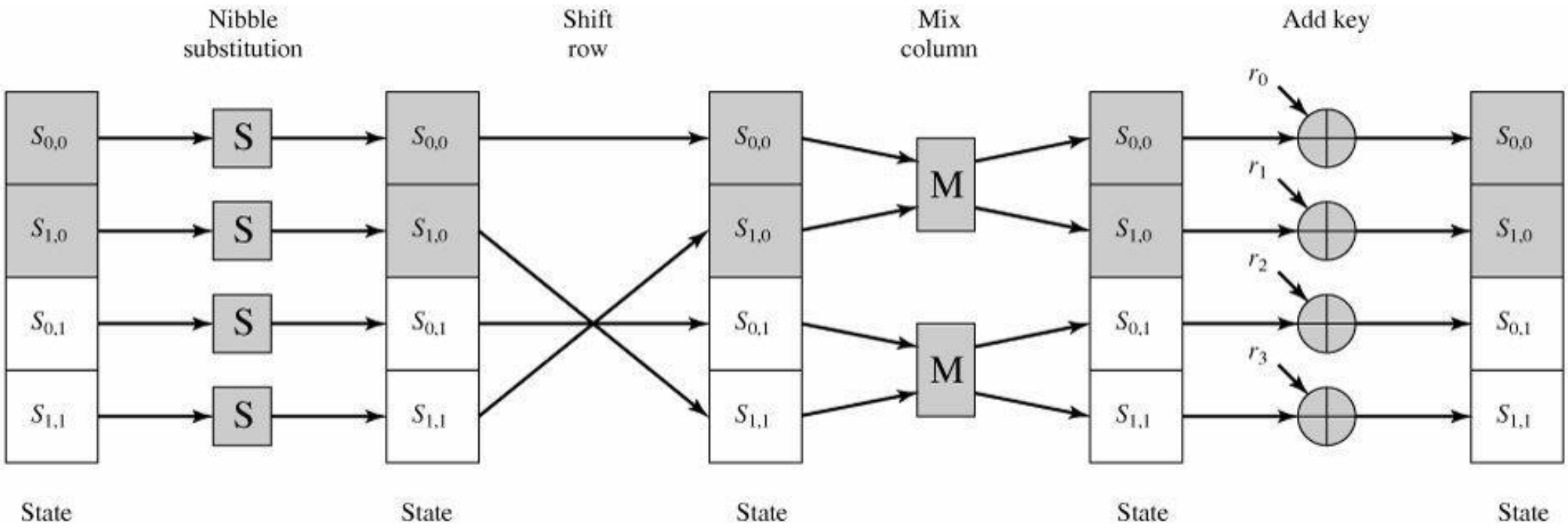


(a) State matrix



(b) Key

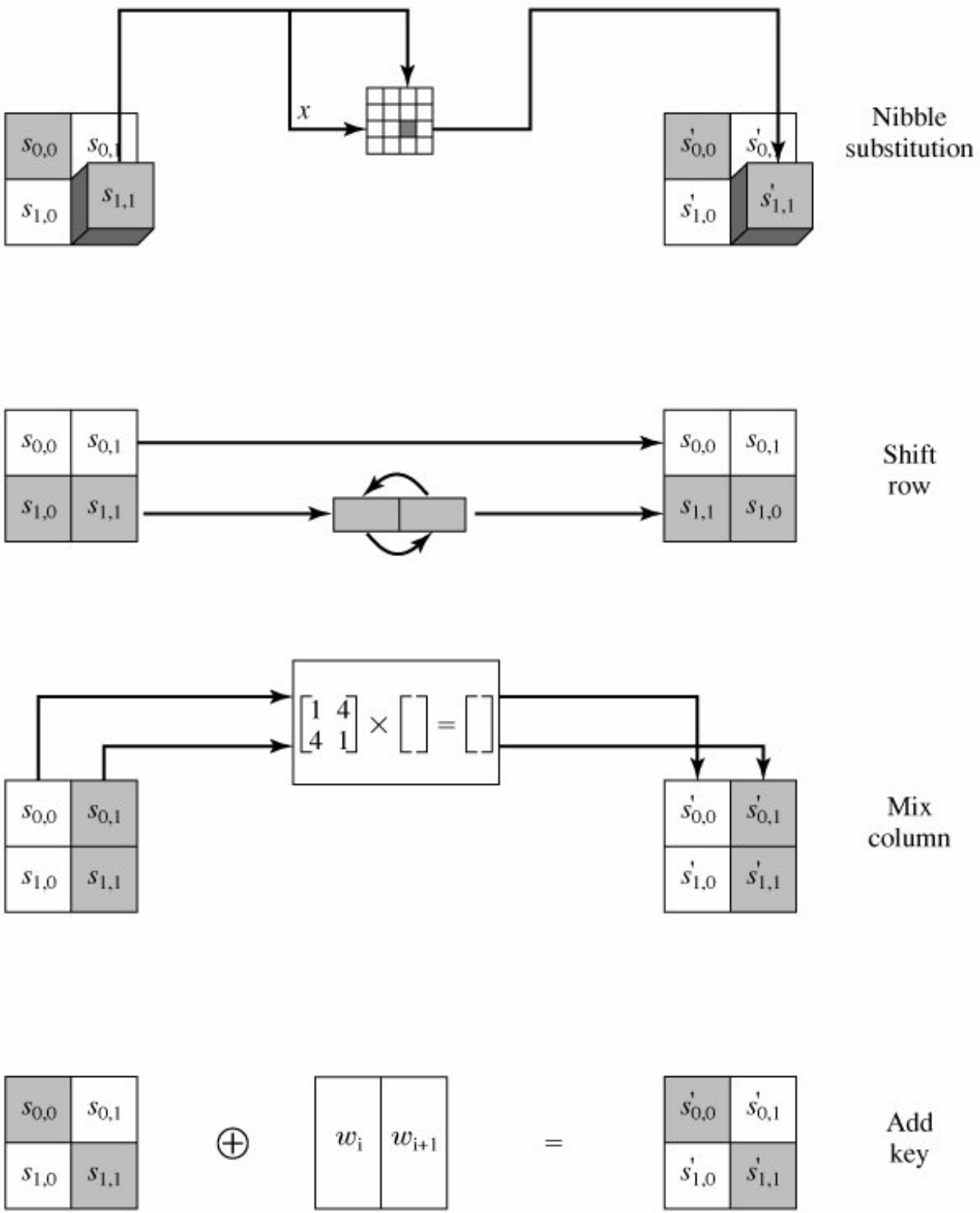
Simplified AES Round



Simplified AES Round Operations

- Nibble Substitution
- Shift Rows
- Mix Columns
- Add Round Key

Simplified AES Round Operations



Simplified AES - S-Box

		j			
		00	**01**	**10**	**11**
i	00	9	4	A	B
	01	D	1	8	5
	10	6	2	0	3
	11	C	E	F	7

(a) S-Box

		j			
		00	**01**	**10**	**11**
i	00	A	5	9	B
	01	1	7	8	F
	10	6	0	2	3
	11	C	4	D	E

(b) Inverse S-Box

Simplified AES - Mix Columns

- Uses Modular Polynomial Arithmetic GF(2^4)

$$m(x) = x^4 + x + 1$$

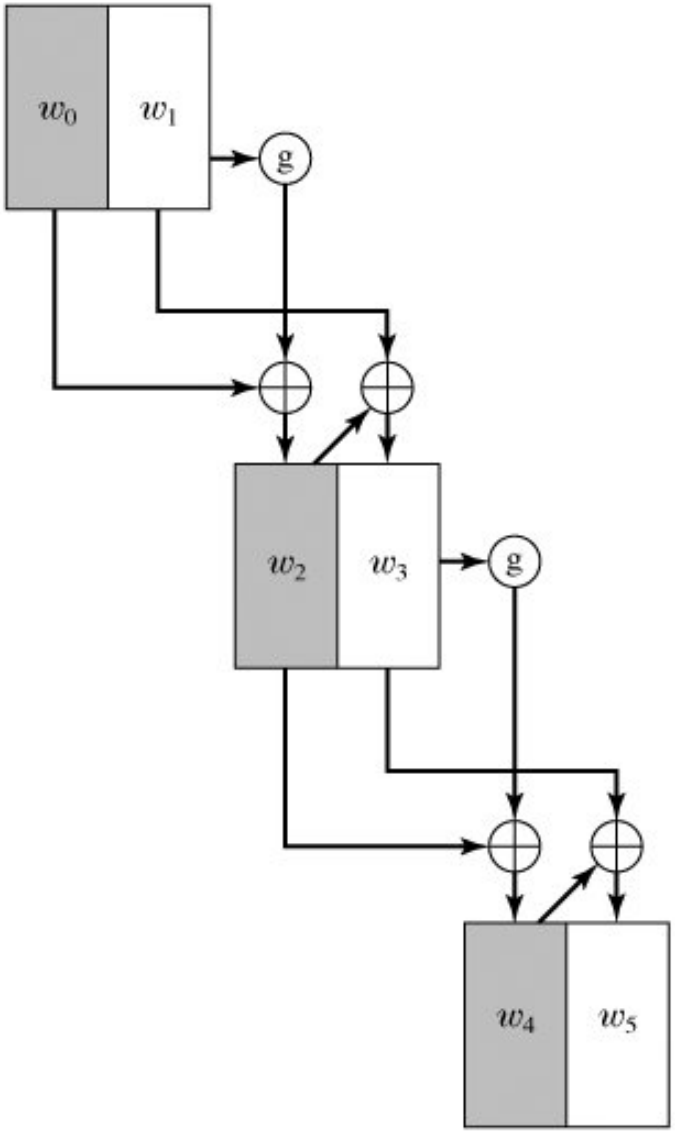
$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} S_{0,0} & S_{0,1} \\ S_{1,0} & S_{1,1} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} \\ S'_{1,0} & S'_{1,1} \end{bmatrix}$$

Forward Mix Columns

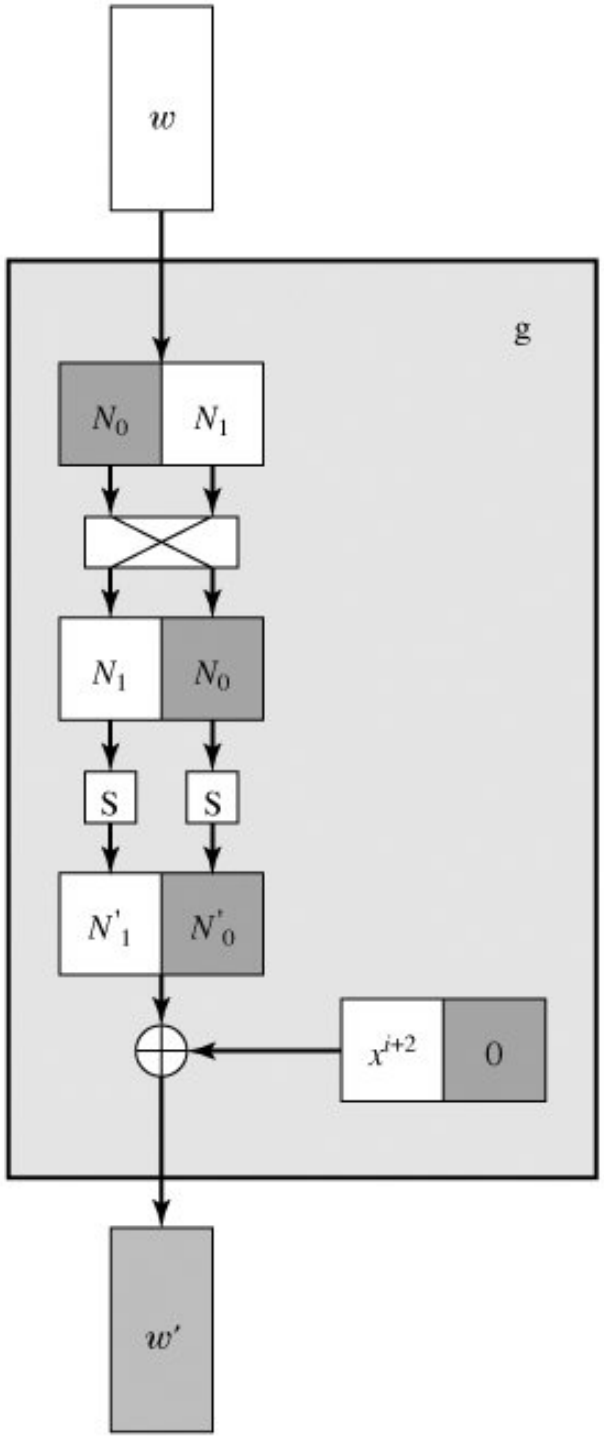
$$\begin{bmatrix} 9 & 2 \\ 2 & 9 \end{bmatrix} \begin{bmatrix} S_{0,0} & S_{0,1} \\ S_{1,0} & S_{1,1} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} \\ S'_{1,0} & S'_{1,1} \end{bmatrix}$$

Inverse Mix Columns

Simplified AES – Key Expansion



(a) Overall algorithm



(b) Function g

Simplified AES – Key Expansion

$$w_0 = [k_0 k_1 k_2 k_3 k_4 k_5 k_6 k_7] \text{ and } w_1 = [k_8 k_9 k_{10} k_{11} k_{12} k_{13} k_{14} k_{15}]$$

$$w_2 = w_0 \oplus g(w_1) = w_0 \oplus RCON(1) \oplus SubNib(RotNib(w_1))$$

$$w_3 = w_1 \oplus w_2$$

$$w_4 = w_2 \oplus g(w_3) = w_2 \oplus RCON(2) \oplus SubNib(RotNib(w_3))$$

$$w_5 = w_3 \oplus w_4$$

$$RCON(i) = [RC[i] \quad 0]$$

$$RC[1] = x^3 \bmod m(x) = 1000$$

$$RC[2] = 2 \cdot RC[1] = x + 1 = 0011$$