# Recall the general structure of AES

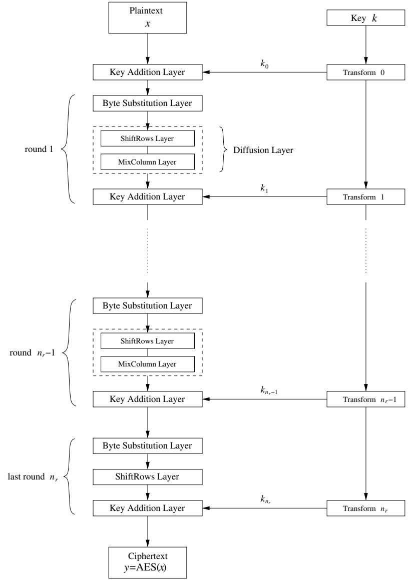


**Fig. 4.2** AES encryption block diagram

# Details of AES round structure

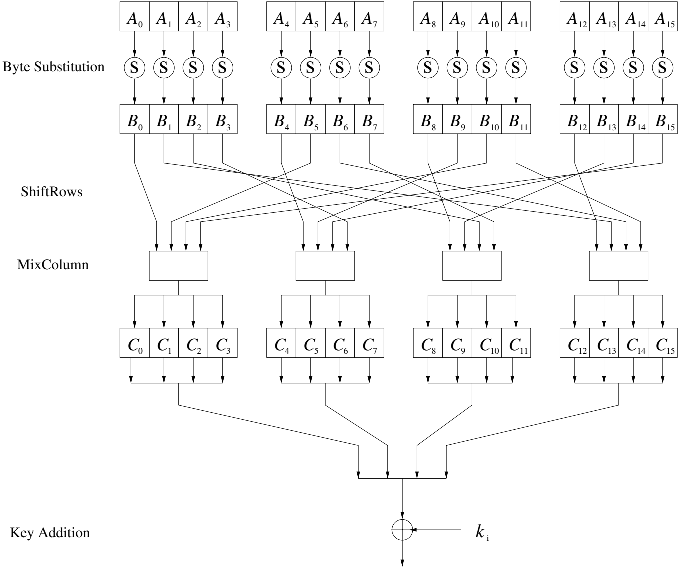
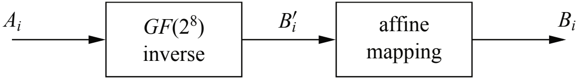

$A_0$ $A_1$ $A_2$ $A_3$ $A_4$ $A_5$ $A_6$ $A_7$ $A_8$ $A_9$ $A_{10}$ $A_{11}$ $A_{12}$ $A_{13}$ $A_{14}$ $A_{15}$
Byte Substitution
S
$B_0$ $B_1$ $B_2$ $B_3$ $B_4$ $B_5$ $B_6$ $B_7$ $B_8$ $B_9$ $B_{10}$ $B_{11}$ $B_{12}$ $B_{13}$ $B_{14}$ $B_{15}$
ShiftRows
MixColumn
$C_0$ $C_1$ $C_2$ $C_3$ $C_4$ $C_5$ $C_6$ $C_7$ $C_8$ $C_9$ $C_{10}$ $C_{11}$ $C_{12}$ $C_{13}$ $C_{14}$ $C_{15}$
Key Addition
$k_i$

**Fig. 4.3** AES round function for rounds $1, 2, \ldots, n_r - 1$

# Format of AES $S$-box



where the affine mapping is

$$MB_i' + v \mod 2$$

where the matrix $M$ and vector $v$ are

$$\underset{\textbf{B\_i}}{\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix}} \equiv \underset{\textbf{M}}{\begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix}} \underset{\textbf{B'\_i}}{\begin{pmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{pmatrix}} + \underset{\textbf{v}}{\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}} \mod 2$$

# The ShiftRows Layer

Place output from byte substitution in a matrix

| | | | |
|---|---|---|---|
| $B_0$ | $B_4$ | $B_8$ | $B_{12}$ |
| $B_1$ | $B_5$ | $B_9$ | $B_{13}$ |
| $B_2$ | $B_6$ | $B_{10}$ | $B_{14}$ |
| $B_3$ | $B_7$ | $B_{11}$ | $B_{15}$ |

Perform the ShiftRows

| | | | | | |
|---|---|---|---|---|---|
| $B_0$ | $B_4$ | $B_8$ | $B_{12}$ | | no shift |
| $B_5$ | $B_9$ | $B_{13}$ | $B_1$ | $\longleftarrow$ | one position left shift |
| $B_{10}$ | $B_{14}$ | $B_2$ | $B_6$ | $\longleftarrow$ | two positions left shift |
| $B_{15}$ | $B_3$ | $B_7$ | $B_{11}$ | $\longleftarrow$ | three positions left shift |

Compare to diagram

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $B_0$ | $B_5$ | $B_{10}$ | $B_{15}$ | $B_4$ | $B_9$ | $B_{14}$ | $B_3$ | $B_8$ | $B_{13}$ | $B_2$ | $B_7$ | $B_{12}$ | $B_1$ | $B_6$ | $B_{11}$ |

# The MixColumns Layer

$$\begin{bmatrix} C_0 & C_4 & C_8 & C_{12} \\ C_1 & C_5 & C_9 & C_{13} \\ C_2 & C_6 & C_{10} & C_{14} \\ C_3 & C_7 & C_{11} & C_{15} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} B_0 & B_4 & B_8 & B_{12} \\ B_5 & B_9 & B_{13} & B_1 \\ B_{10} & B_{14} & B_2 & B_6 \\ B_{15} & B_3 & B_7 & B_{11} \end{bmatrix}$$

Notice that all operations in the matrix multiplication are taking place in $GF(2^8)$

# Diffusion Layer Example

Suppose output of byte substitution layer is

| $B_0$ | $B_1$ | $B_2$ | $B_3$ | $B_4$ | $B_5$ | $B_6$ | $B_7$ | $B_8$ | $B_9$ | $B_{10}$ | $B_{11}$ | $B_{12}$ | $B_{13}$ | $B_{14}$ | $B_{15}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5E | 62 | 1F | 03 | 77 | 4E | 39 | 06 | 48 | 2A | 35 | 2C | 52 | 01 | 11 | 20 |

ShiftRows:

$$\begin{bmatrix} 5E & 77 & 48 & 52 \\ 62 & 4E & 2A & 01 \\ 1F & 39 & 35 & 11 \\ 03 & 06 & 2C & 20 \end{bmatrix} \Rightarrow \begin{bmatrix} 5E & 77 & 48 & 52 \\ 4E & 2A & 01 & 62 \\ 35 & 11 & 1F & 39 \\ 20 & 03 & 06 & 2C \end{bmatrix}$$

MixColumns:

$$\begin{bmatrix} C_0 & C_4 & C_8 & C_{12} \\ C_1 & C_5 & C_9 & C_{13} \\ C_2 & C_6 & C_{10} & C_{14} \\ C_3 & C_7 & C_{11} & C_{15} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 5E & 77 & 48 & 52 \\ 4E & 2A & 01 & 62 \\ 35 & 11 & 1F & 39 \\ 20 & 03 & 06 & 2C \end{bmatrix}$$

# The 128-bit AES Key Schedule

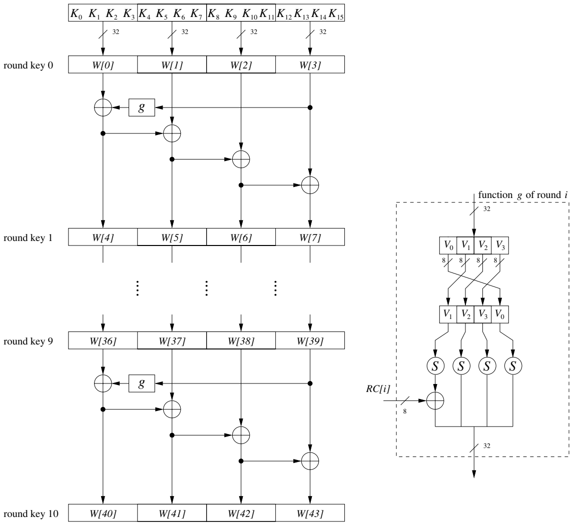
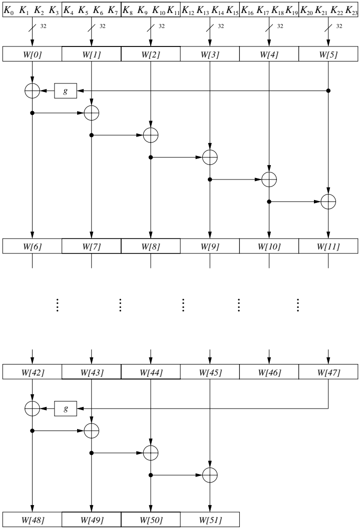


**Fig. 4.5** AES key schedule for 128-bit key size

$$RC[i] = x^i$$

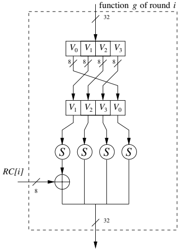
Need to generate 44 words of 32-bits each

# The 192-bit AES Key Schedule



$K_0$ $K_1$ $K_2$ $K_3$ $K_4$ $K_5$ $K_6$ $K_7$ $K_8$ $K_9$ $K_{10}$ $K_{11}$ $K_{12}$ $K_{13}$ $K_{14}$ $K_{15}$ $K_{16}$ $K_{17}$ $K_{18}$ $K_{19}$ $K_{20}$ $K_{21}$ $K_{22}$ $K_{23}$
32
W[0] W[1] W[2] W[3] W[4] W[5]
g
W[6] W[7] W[8] W[9] W[10] W[11]
W[42] W[43] W[44] W[45] W[46] W[47]
g
W[48] W[49] W[50] W[51]

**Fig. 4.6** AES key schedule for 192-bit key sizes



$$RC[i] = x^i$$

Need to generate 52 words of 32-bits each

# The 256-bit AES Key Schedule

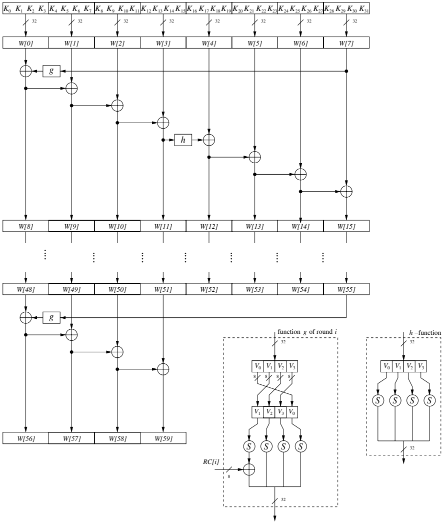

K0 K1 K2 K3 K4 K5 K6 K7 K8 K9 K10 K11 K12 K13 K14 K15 K16 K17 K18 K19 K20 K21 K22 K23 K24 K25 K26 K27 K28 K29 K30 K31
32
W[0] W[1] W[2] W[3] W[4] W[5] W[6] W[7]
g
h
W[8] W[9] W[10] W[11] W[12] W[13] W[14] W[15]
W[48] W[49] W[50] W[51] W[52] W[53] W[54] W[55]
g
W[56] W[57] W[58] W[59]
function g of round i
V0 V1 V2 V3
8
V1 V2 V3 V0
S S S S
RC[i]
8
32
h –function
V0 V1 V2 V3
S S S S
32

**Fig. 4.7** AES key schedule for 256-bit key size

$$RC[i] = x^i$$

Need to generate 60 words of 32-bits each