

$\mathbb{F}_{2^8} \ni a = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7,$

where $a_i \in \mathbb{F}_2 = \{0, 1\}$.

Representation: 8 bits for an element = 1 byte.

Addition: XOR, $(a + b)_i = a_i + b_i$.

Multiplication: as for polynomials modulo $x^8 + x^4 + x^3 + x + 1$.

Example $57 \cdot 83 = C1$:

$$\begin{aligned} (x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1) &= x^{13} + x^{11} + x^9 + x^8 + x^7 + \\ &\quad x^7 + x^5 + x^3 + x^2 + x + \\ &\quad x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\ &= x^7 + x^6 + 1 \pmod{x^8 + x^4 + x^3 + x + 1}. \end{aligned}$$

Field: You can divide by every non-zero element.

Figure 1: The field \mathbb{F}_{2^8}

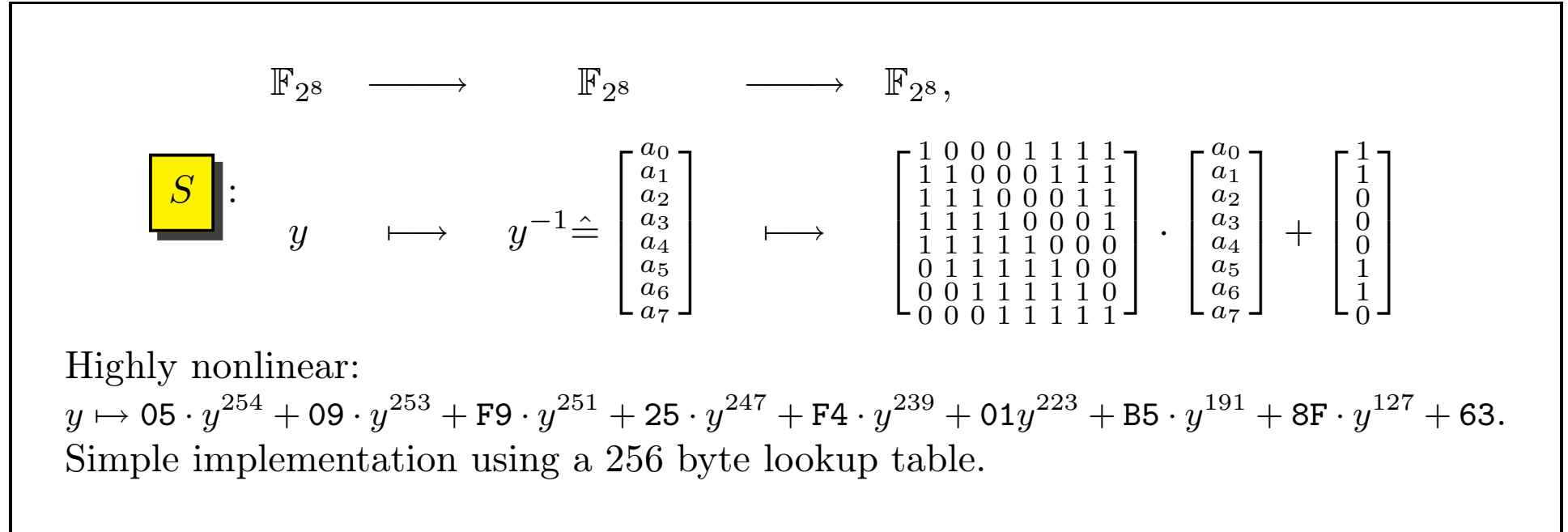


Figure 2: The S-Box

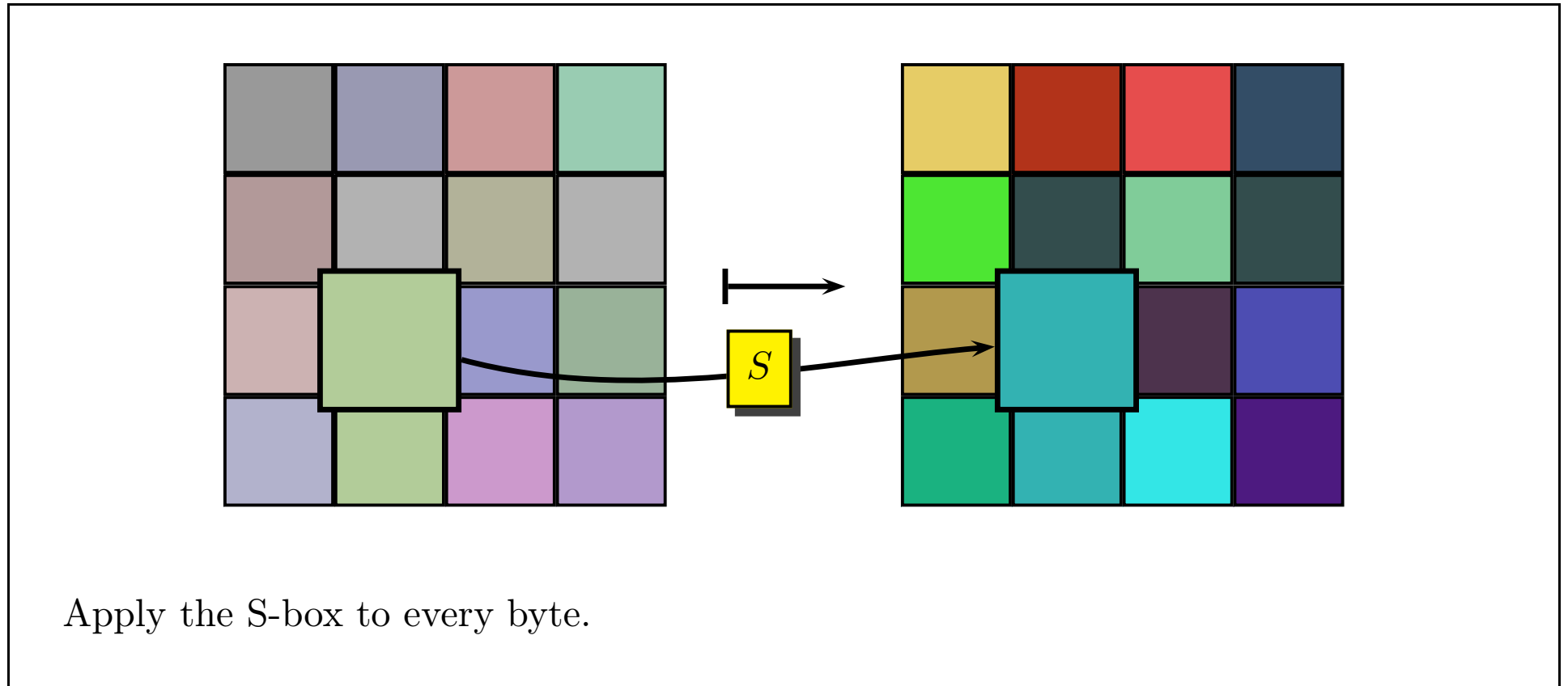
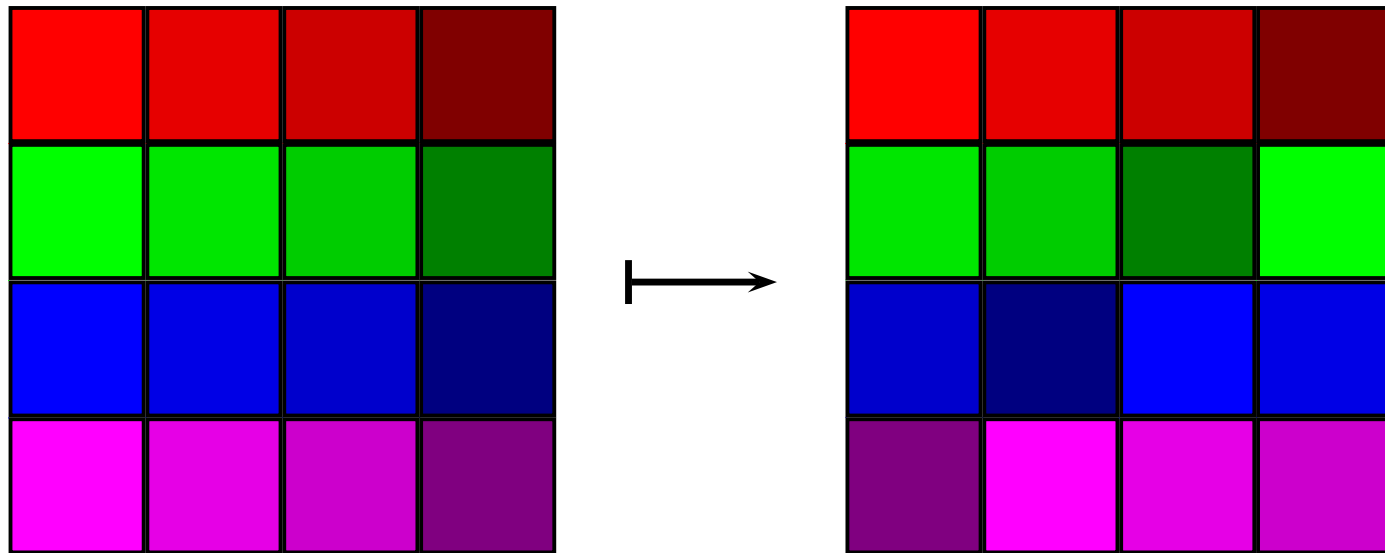


Figure 3: The SubBytes operation



The rows are shifted cyclically by zero, one, two, or three bytes.

Figure 4: The ShiftRows operation

$R = \mathbb{F}_{2^8}[z]/(z^4 + 1) \ni a_0 + a_1z + a_2z^2 + a_3z^3,$

where $a_i \in \mathbb{F}_{2^8}$.

Addition: coefficient-wise $(a + b)_i = a_i + b_i$, XOR.

Multiplication: as for polynomials modulo $z^4 + 1$. Another way to express $d = a \cdot b$ is by the following matrix equation:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Not a field: $(z + 1)^4 = 0$.

Figure 5: Polynomials over the field \mathbb{F}_{2^8}

$$R = \mathbb{F}_{2^8}[z]/(z^4 + 1) \ni a_0 + a_1z + a_2z^2 + a_3z^3,$$

where $a_i \in \mathbb{F}_{2^8}$.

Addition: coefficient-wise $(a + b)_i = a_i + b_i$, XOR.

Multiplication: as for polynomials modulo $z^4 + 1$. Another way to express $d = a \cdot b$ is by the following matrix equation:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Not a field: $(z + 1)^4 = 0$.

Figure 5: Polynomials over the field \mathbb{F}_{2^8}

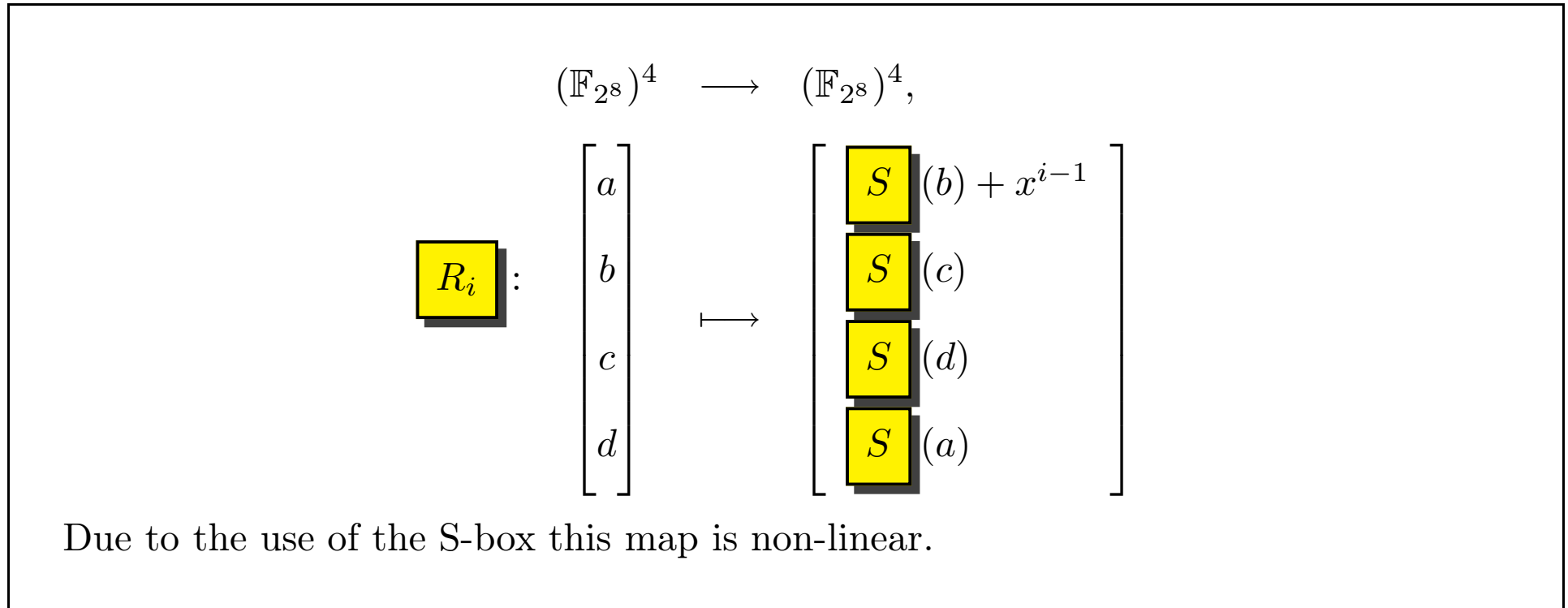


Figure 7: Nonlinear part of the key schedule

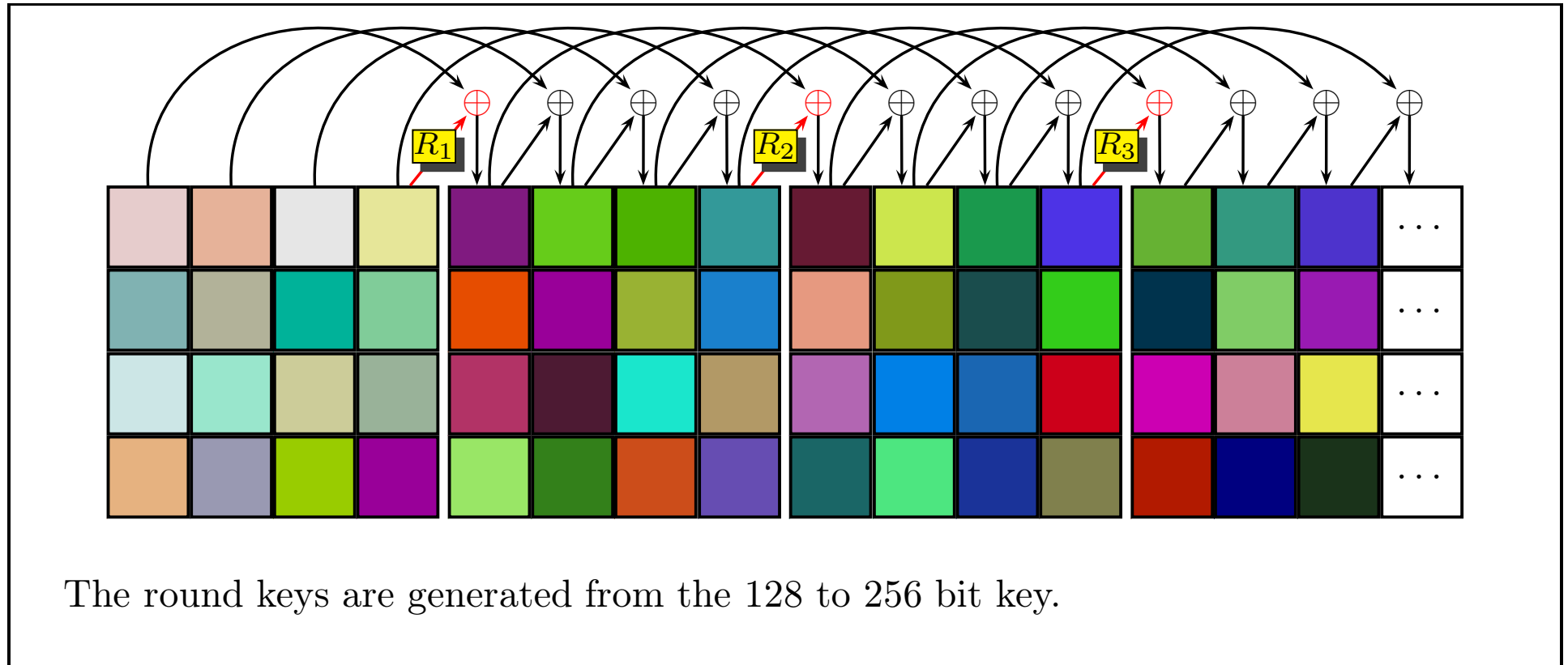
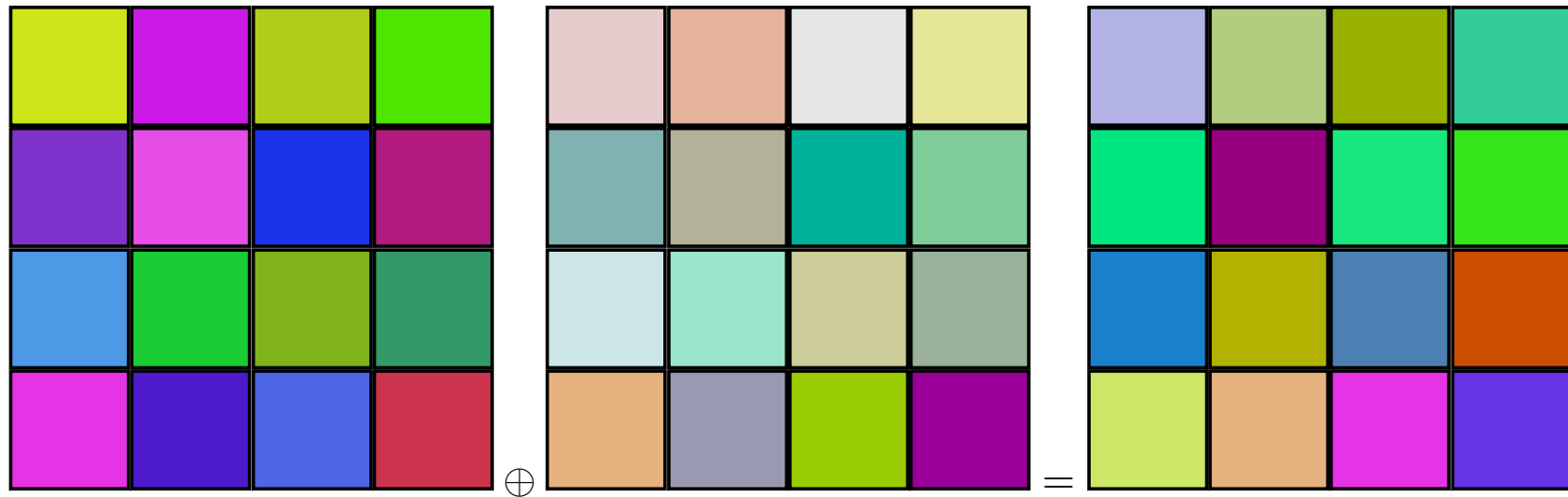


Figure 8: The Key Schedule



Simple XOR with the round key.

Figure 9: The AddRoundKey operation

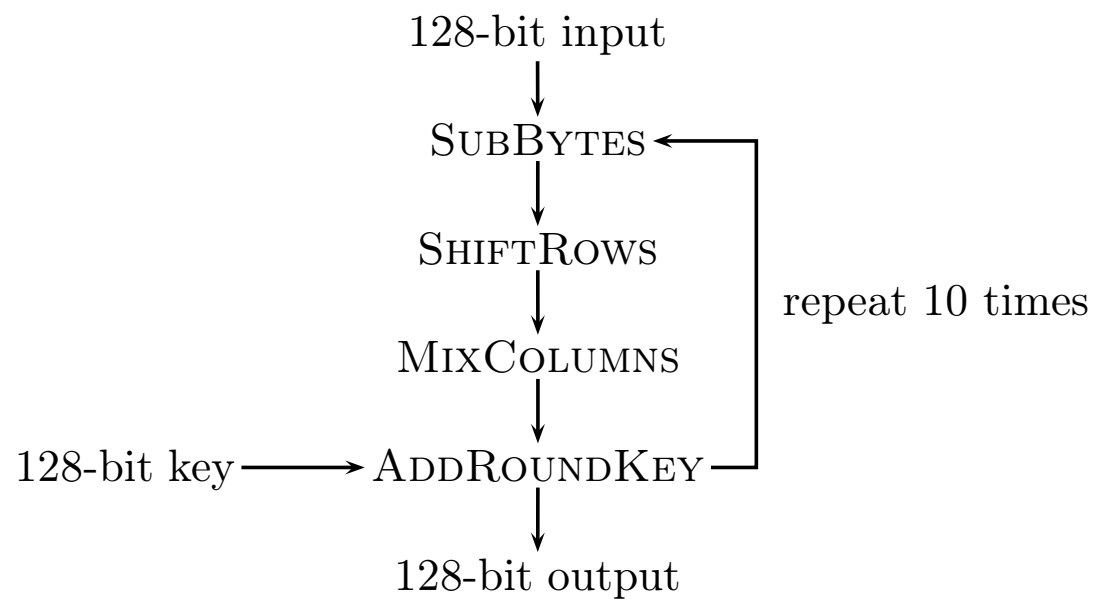


Figure 10: The overall structure of *AES!* (**AES!**)