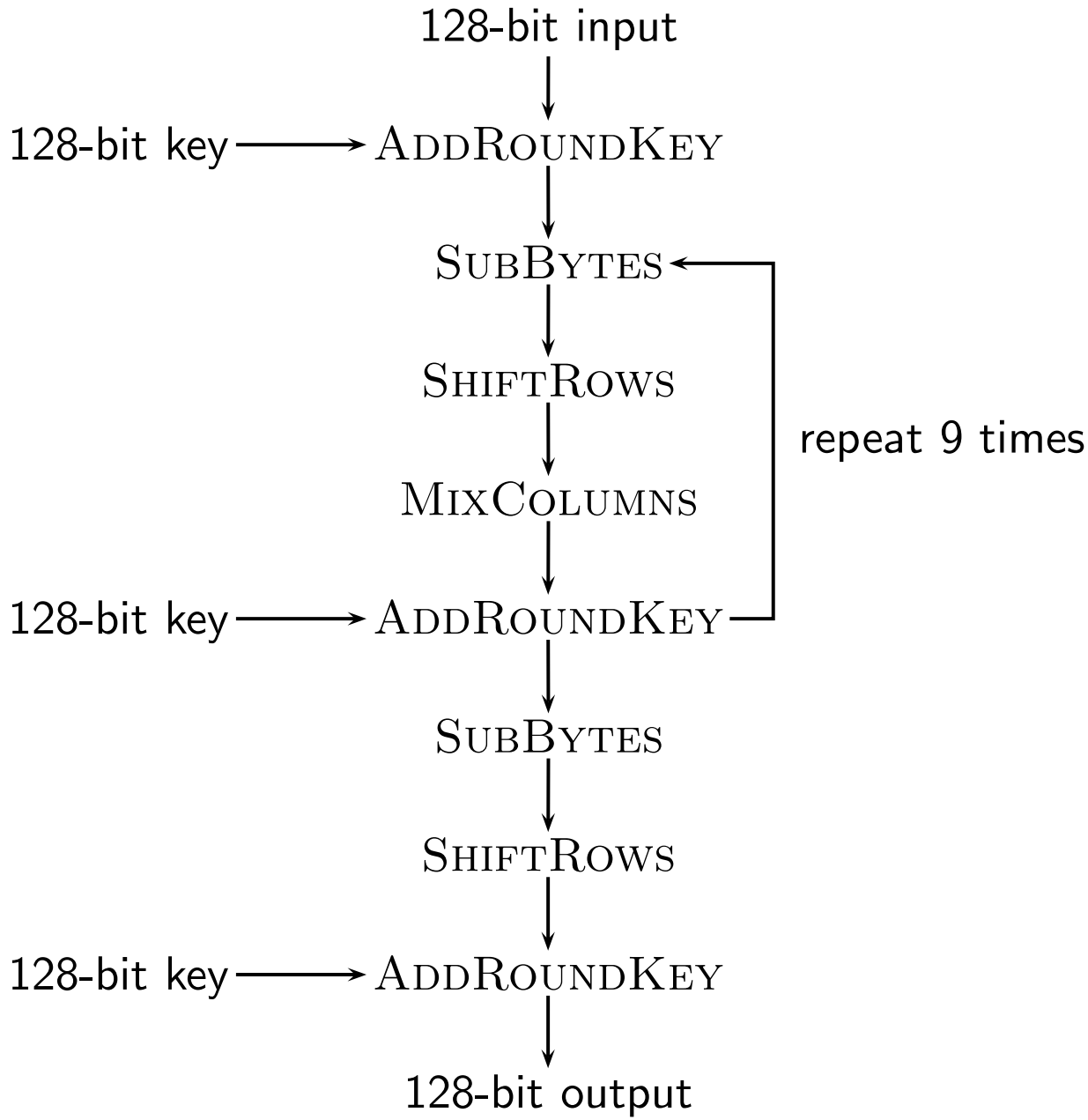
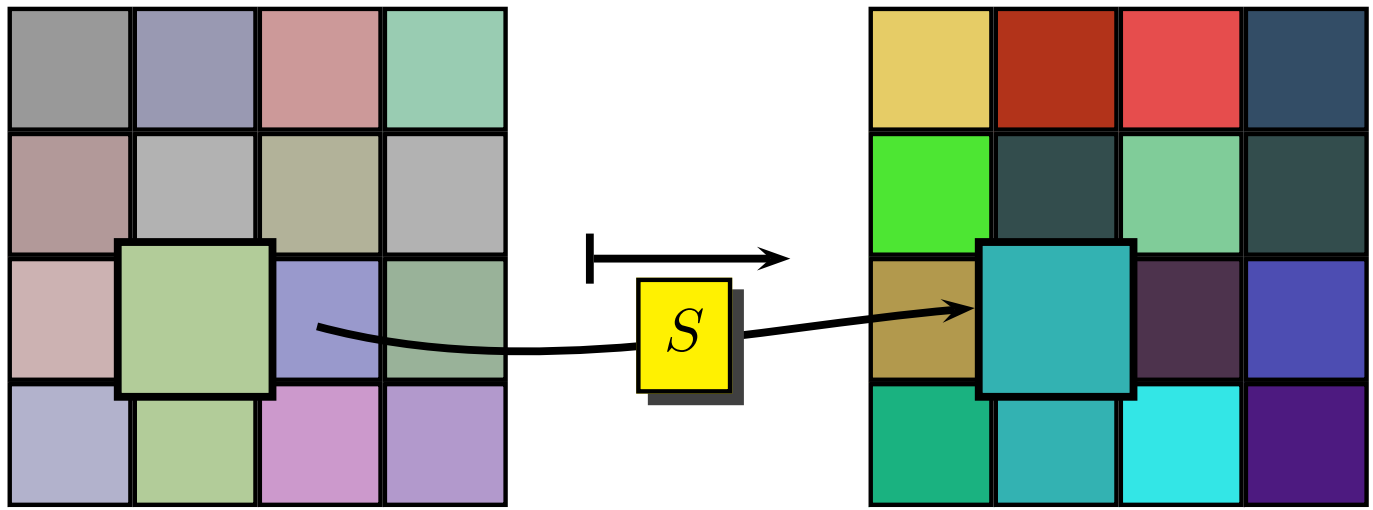
Cryptography, winter 2014/15

The Advanced Encryption Standard

Dr. Daniel Loebenberger


128-bit input
128-bit key
AddRoundKey
SubBytes
ShiftRows
MixColumns
repeat 9 times
128-bit key
AddRoundKey
SubBytes
ShiftRows
128-bit key
AddRoundKey
128-bit output



Applying SubBytes to every byte.

$\mathbb{F}_{256} = \mathbb{F}_{2^8} \ni a = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7$,
with all $a_i \in \mathbb{F}_2 = \{0, 1\}$.
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 $57 \cdot 83 = \mathtt{C1}$:

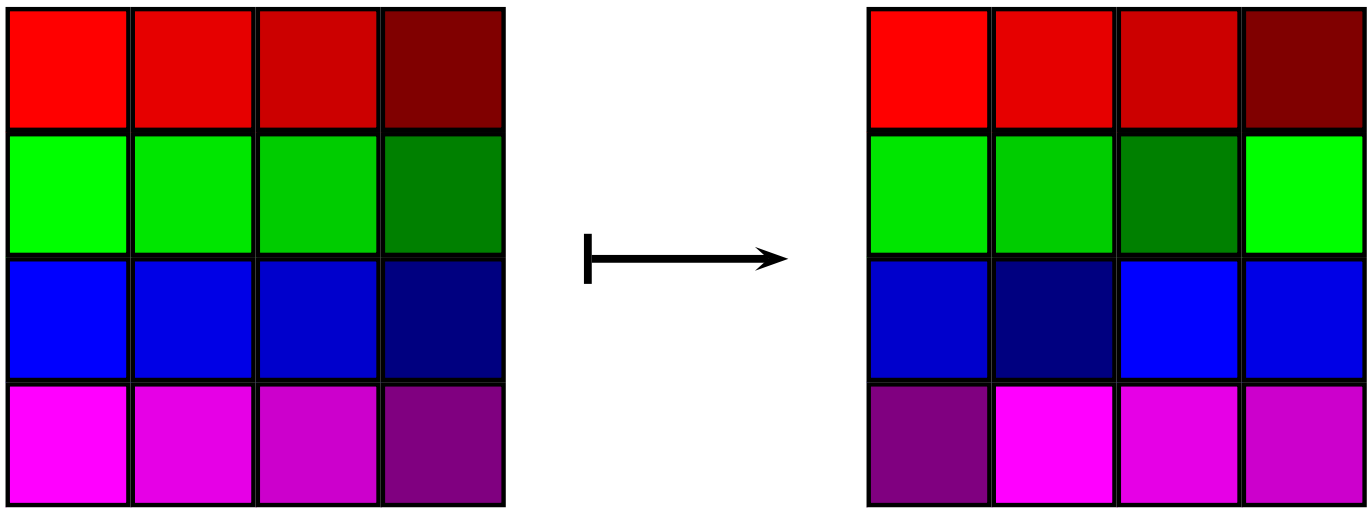
$$
\begin{aligned}
&(x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1) \\
&\quad = x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 + x^5 \\
&\qquad + x^3 + x^2 + x + x^6 + x^4 + x^2 + x + 1 \\
&\quad = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \text{ in } \mathbb{Z}_2[x] \\
&\quad = x^7 + x^6 + 1 \text{ in } \mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1).
\end{aligned}
$$

$$\mathbb{F}_{256} \longrightarrow \mathbb{F}_{256} \longrightarrow \mathbb{F}_{256},$$

S:

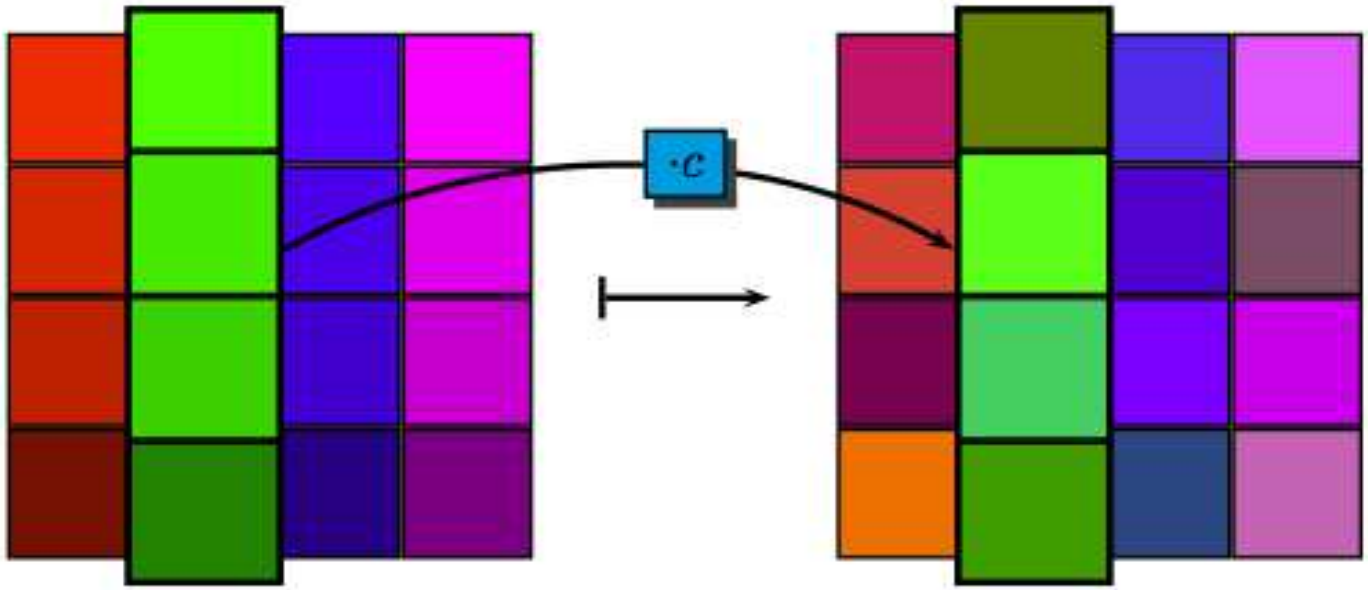
$$a \longmapsto \mathsf{inv}(a) = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \longmapsto \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$a \mapsto \mathtt{05} \cdot a^{254} + \mathtt{09} \cdot a^{253} + \mathtt{F9} \cdot a^{251} + \mathtt{25} \cdot a^{247} + \mathtt{F4} \cdot a^{239} + \mathtt{01} \cdot a^{223} + \mathtt{B5} \cdot a^{191} + \mathtt{8F} \cdot a^{127} + \mathtt{63}.$



The four rows are shifted cyclically to the left by zero, one, two, and three bytes, respectively.

$$\begin{matrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{matrix} \mapsto \begin{matrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{11} & a_{12} & a_{13} & a_{10} \\ a_{22} & a_{23} & a_{20} & a_{21} \\ a_{33} & a_{30} & a_{31} & a_{32} \end{matrix}$$



Each column is considered as an element of $\mathbb{F}_{256}[y]/(y^4+1)$
and multiplied by $c = \mathtt{02} + \mathtt{01}y + \mathtt{01}y^2 + \mathtt{03}y^3$.
Inverse: Multiply with $d = \mathtt{0E} + \mathtt{09}y + \mathtt{0D}y^2 + \mathtt{0B}y^3$.

$R = \mathbb{F}_{256}[z]/(z^4+1) \ni a_0 + a_1 z + a_2 z^2 + a_3 z^3$, with all $a_i \in \mathbb{F}_{256}$.

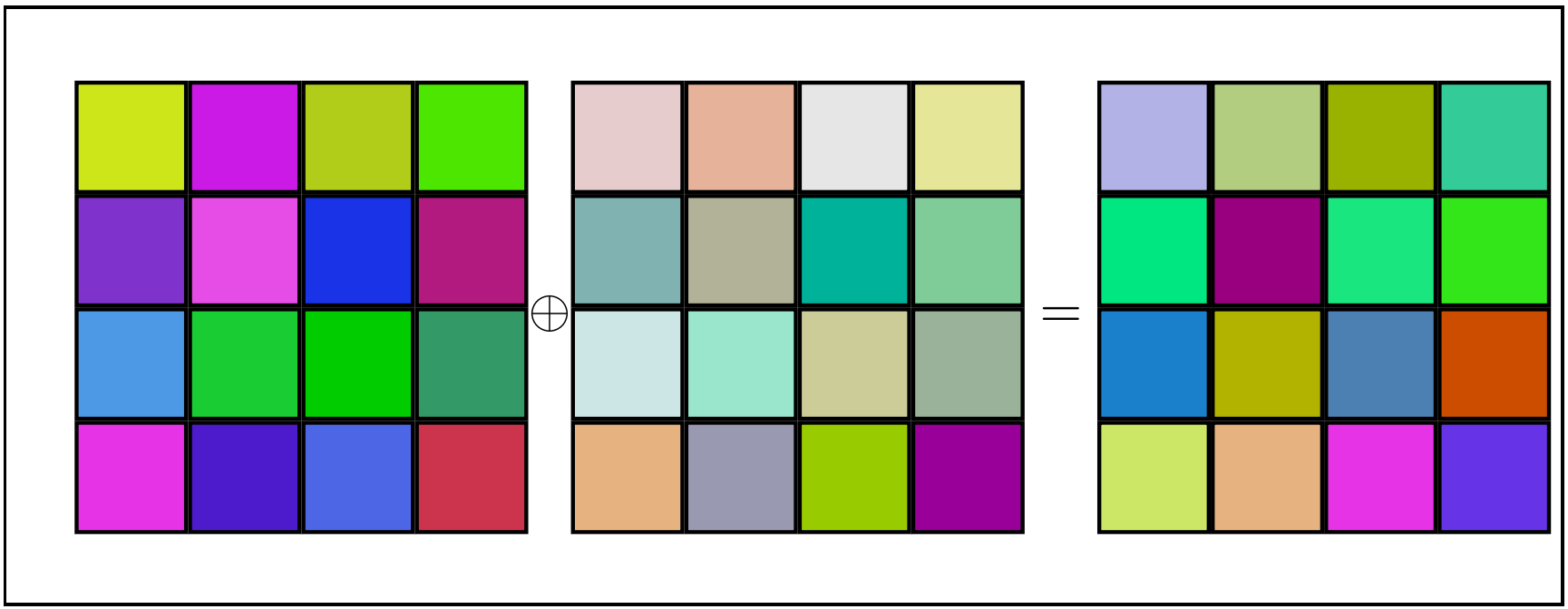
Addition: coefficient-wise $(a+b)_i = a_i + b_i$.

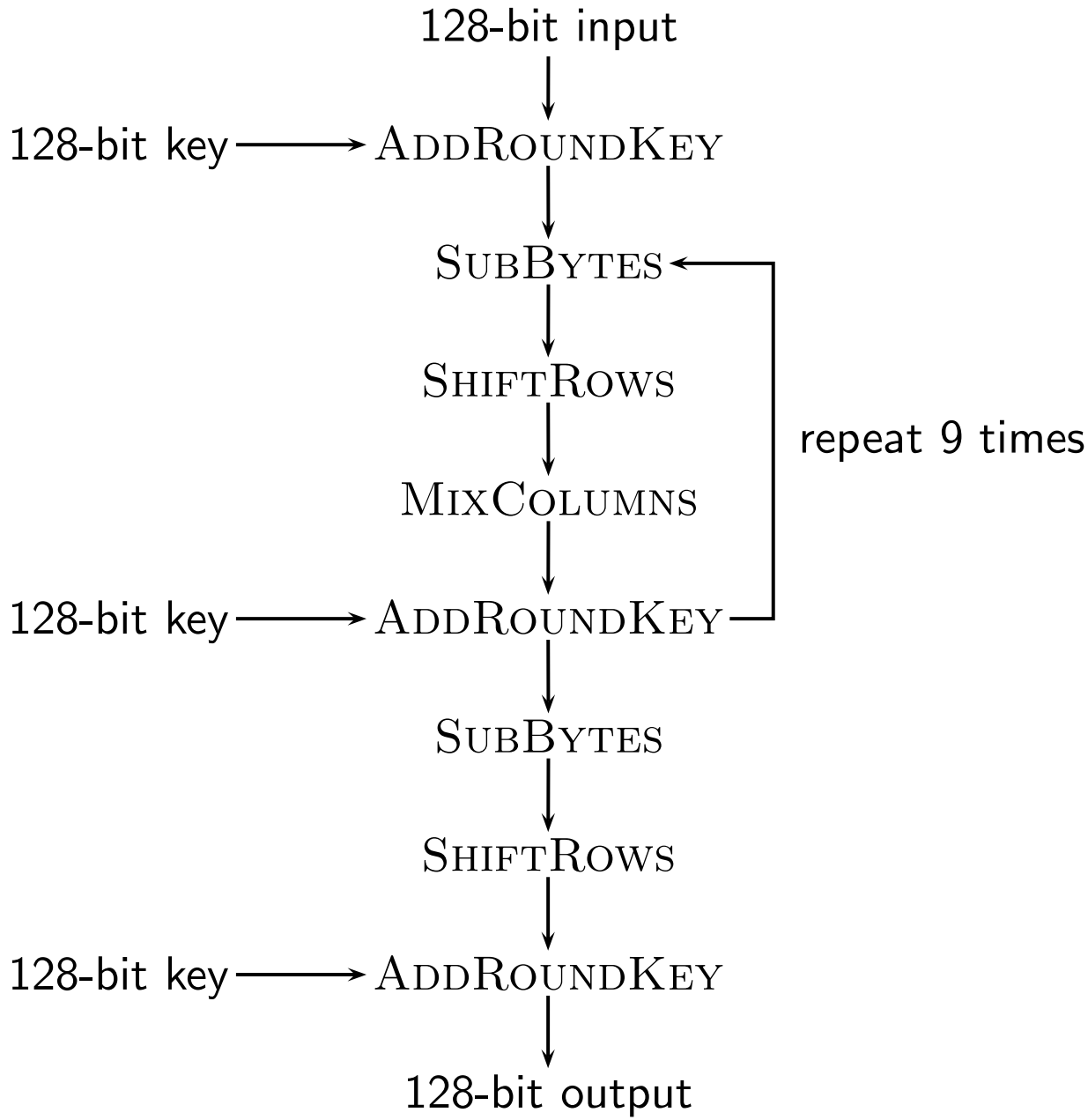
Multiplication: modulo $z^4 + 1$.

The multiplication $d = a \cdot b$ in R can be expressed by the following matrix equation over $\mathbb{F}_{256}$:

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

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$$




128-bit input
128-bit key
AddRoundKey
SubBytes
ShiftRows
MixColumns
repeat 9 times
128-bit key
AddRoundKey
SubBytes
ShiftRows
128-bit key
AddRoundKey
128-bit output

key length		
in bits	in ℓ_k words	ℓ_r rounds
128	4	10
196	6	12
256	8	14

AES allows keys of 128, 196, or 256 bits, which corresponds to ℓ_k many 32-bit words for $\ell_k = 4$, 6, or 8. The ℓ_r is the number of rounds after the initial one.