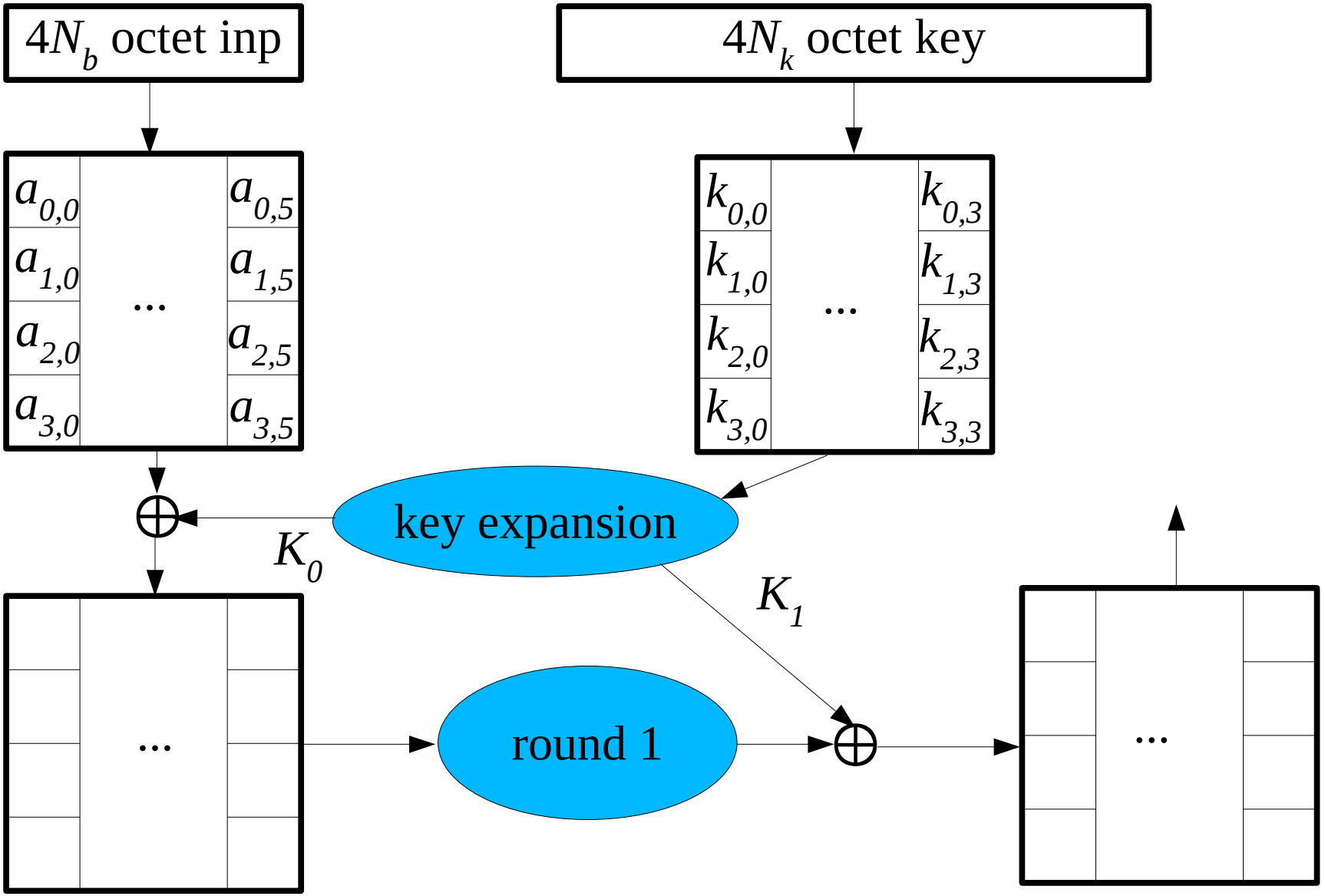
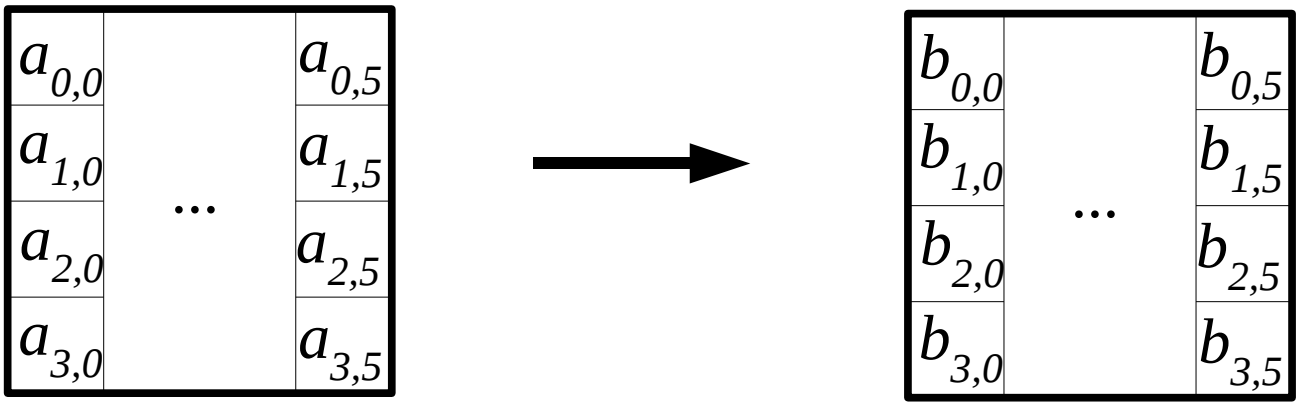
Secret Key Systems - AES

NIST (2001) parameterized key size (128 bits to 256 bits)



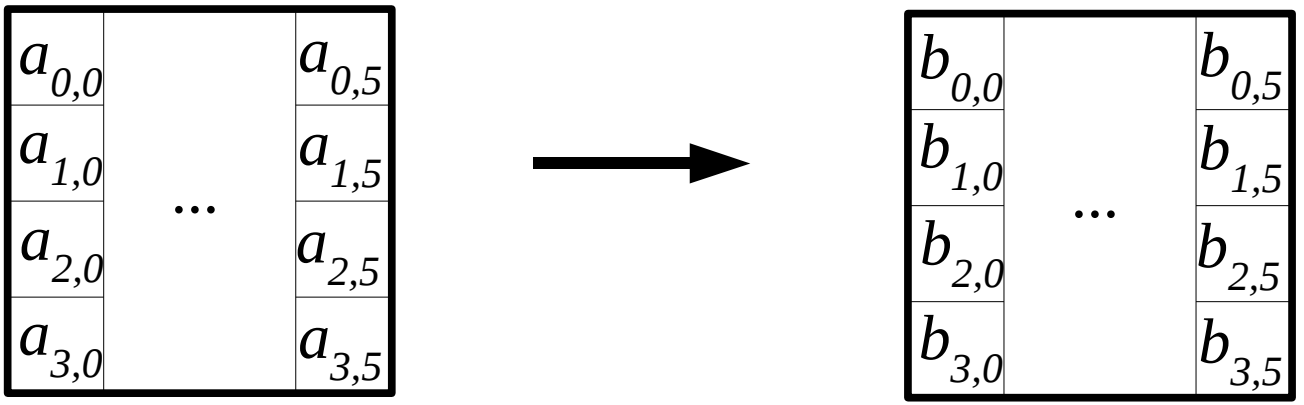
Secret Key Systems - AES

1. Byte Substitution via S-box - the transformation is invertable



Secret Key Systems - AES

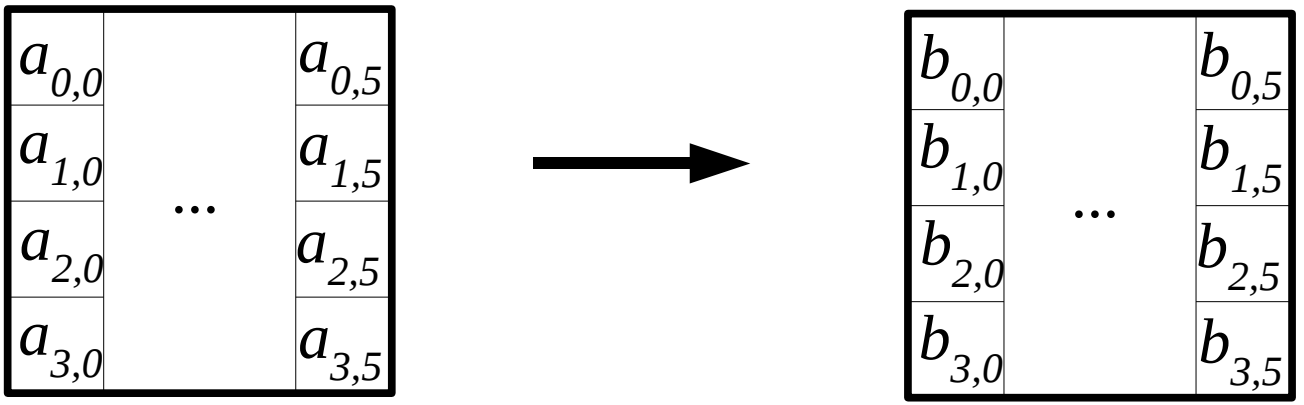
1. Byte Substitution via S-box - the transformation is invertable



A byte as a polynomial: $b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$, $b_i \in \{0,1\}$

Secret Key Systems - AES

1. Byte Substitution via S-box - the transformation is invertable

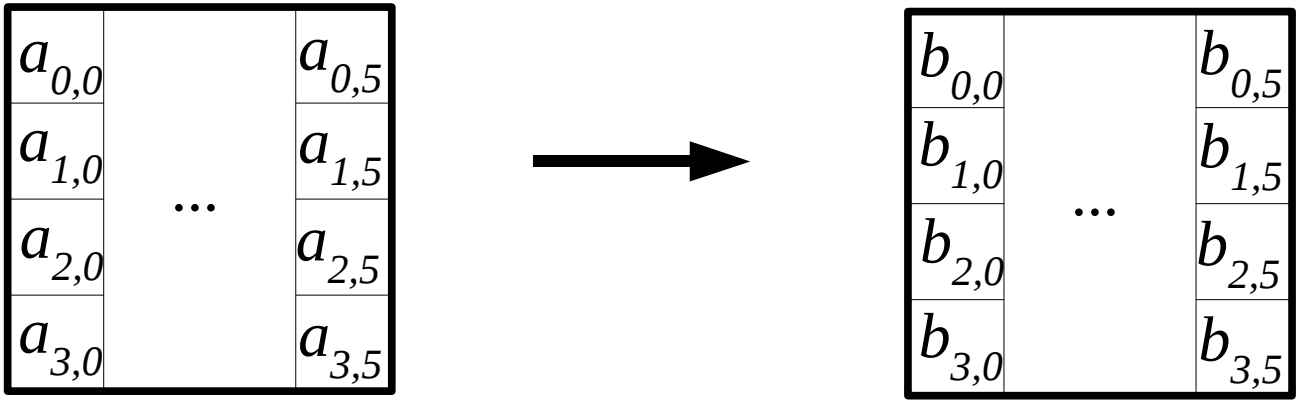


A byte as a polynomial: $b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$, $b_i \in \{0,1\}$

Addition: $(x^6+x^4+x^2+x^1+1) + (x^7+x^1+1) = x^7+x^6+x^4+x^2$ (exclusive or)

Secret Key Systems - AES

1. Byte Substitution via S-box - the transformation is invertable



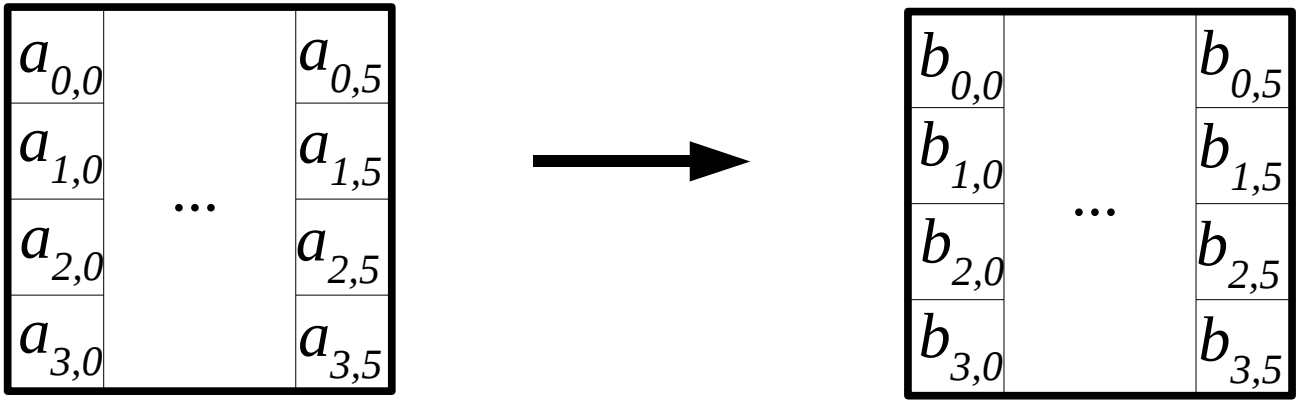
A byte as a polynomial: $b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$, $b_i \in \{0,1\}$

Addition: $(x^6+x^4+x^2+x^1+1) + (x^7+x^1+1) = x^7+x^6+x^4+x^2$ (exclusive or)

Multiplication: $(x^6+x^4+x^2+x^1+1)*(x^7+x^1+1) =$
$x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+x^1+1$

Secret Key Systems - AES

1. Byte Substitution via S-box - the transformation is invertable



A byte as a polynomial: $b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$, $b_i \in \{0,1\}$

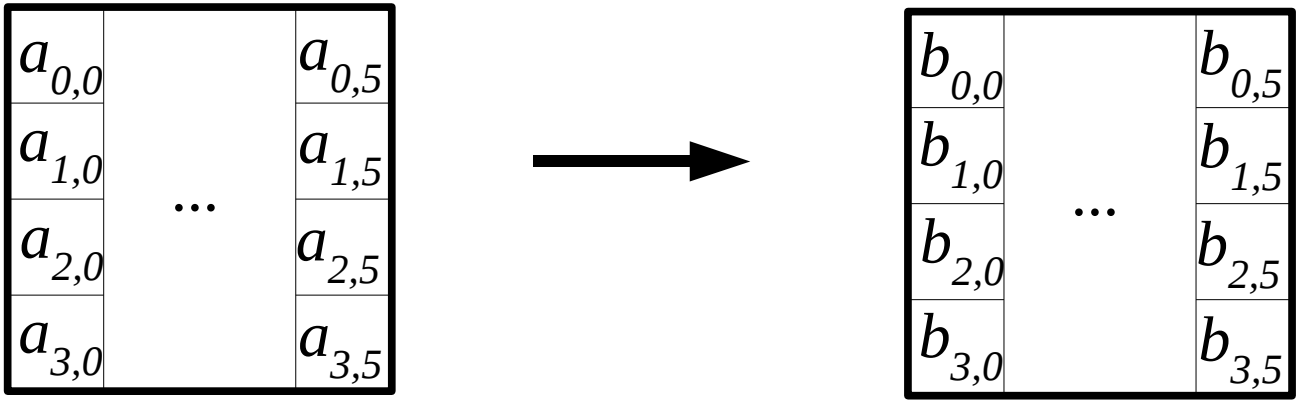
Addition: $(x^6+x^4+x^2+x^1+1) + (x^7+x^1+1) = x^7+x^6+x^4+x^2$ (exclusive or)

Multiplication: $(x^6+x^4+x^2+x^1+1)*(x^7+x^1+1) =$
$x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+x^1+1$

Irreducible polynomial: $m(x) = x^8+x^4+x^3+x^1+1$

Secret Key Systems - AES

1. Byte Substitution via S-box - the transformation is invertable



A byte as a polynomial: $b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$, $b_i \in \{0,1\}$

Addition: $(x^6+x^4+x^2+x^1+1) + (x^7+x^1+1) = x^7+x^6+x^4+x^2$ (exclusive or)

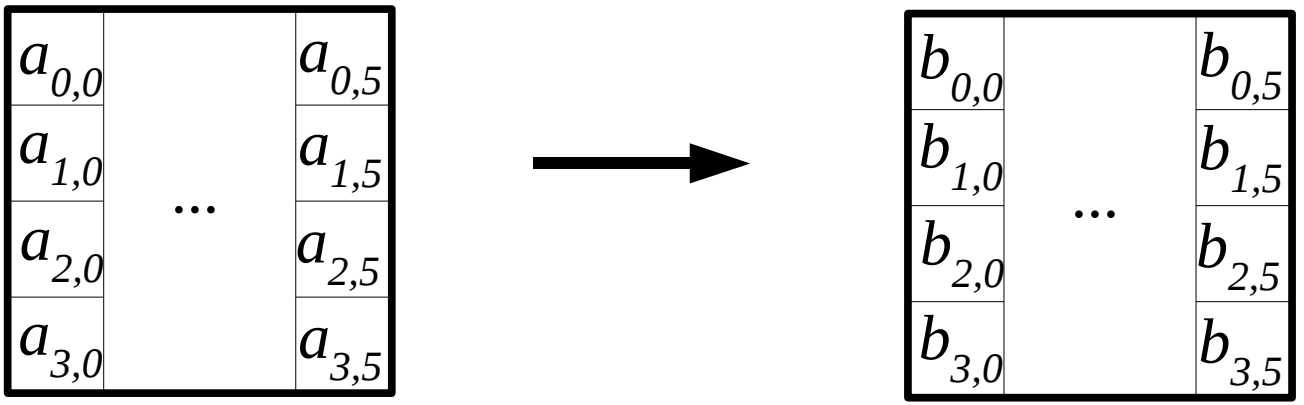
Multiplication: $(x^6+x^4+x^2+x^1+1)*(x^7+x^1+1) = x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+x^1+1$

Irreducible polynomial: $m(x) = x^8+x^4+x^3+x^1+1$

Multiplication mod m(x): $(x^6+x^4+x^2+x^1+1)*(x^7+x^1+1) \bmod m(x) = x^7+x^6+1$

Secret Key Systems - AES

1. Byte Substitution via S-box - the transformation is invertable



A byte as a polynomial: $b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$, $b_i \in \{0,1\}$

Addition: $(x^6+x^4+x^2+x^1+1) + (x^7+x^1+1) = x^7+x^6+x^4+x^2$ (exclusive or)

Multiplication: $(x^6+x^4+x^2+x^1+1)*(x^7+x^1+1) =$
$x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+x^1+1$

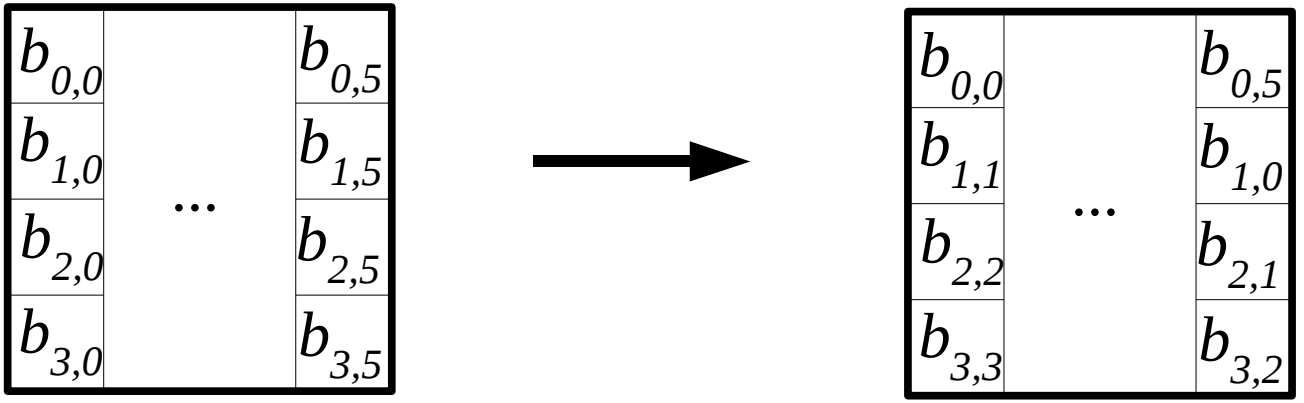
Irreducible polynomial: $m(x) = x^8+x^4+x^3+x^1+1$

Multiplication mod m(x): $(x^6+x^4+x^2+x^1+1)*(x^7+x^1+1) \bmod m(x) = x^7+x^6+1$

Use Euclid's algorithm to compute, for any b(x): $b(x)*a(x) + c(x)*m(x) = 1$
That is, b(x) and a(x) are inverses modulo m(x): $b^{-1}(x) = a(x) \bmod m(x)$
This defines the S-box.

Secret Key Systems - AES

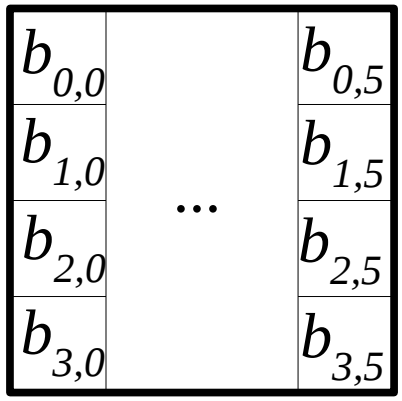
2. Row shift (cycle, left)

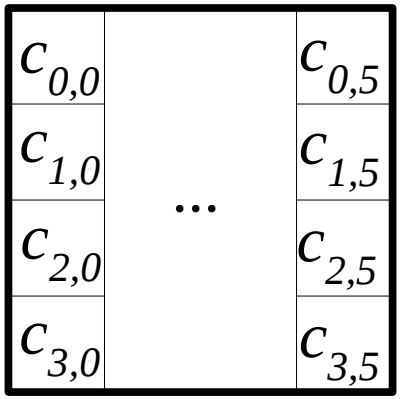


N_b \ Row	1	2	3
4	1	2	3
6	1	2	3
8	1	3	4

Secret Key Systems - AES

3. Mixed Column Transformation – constants are 8 bits now





E:

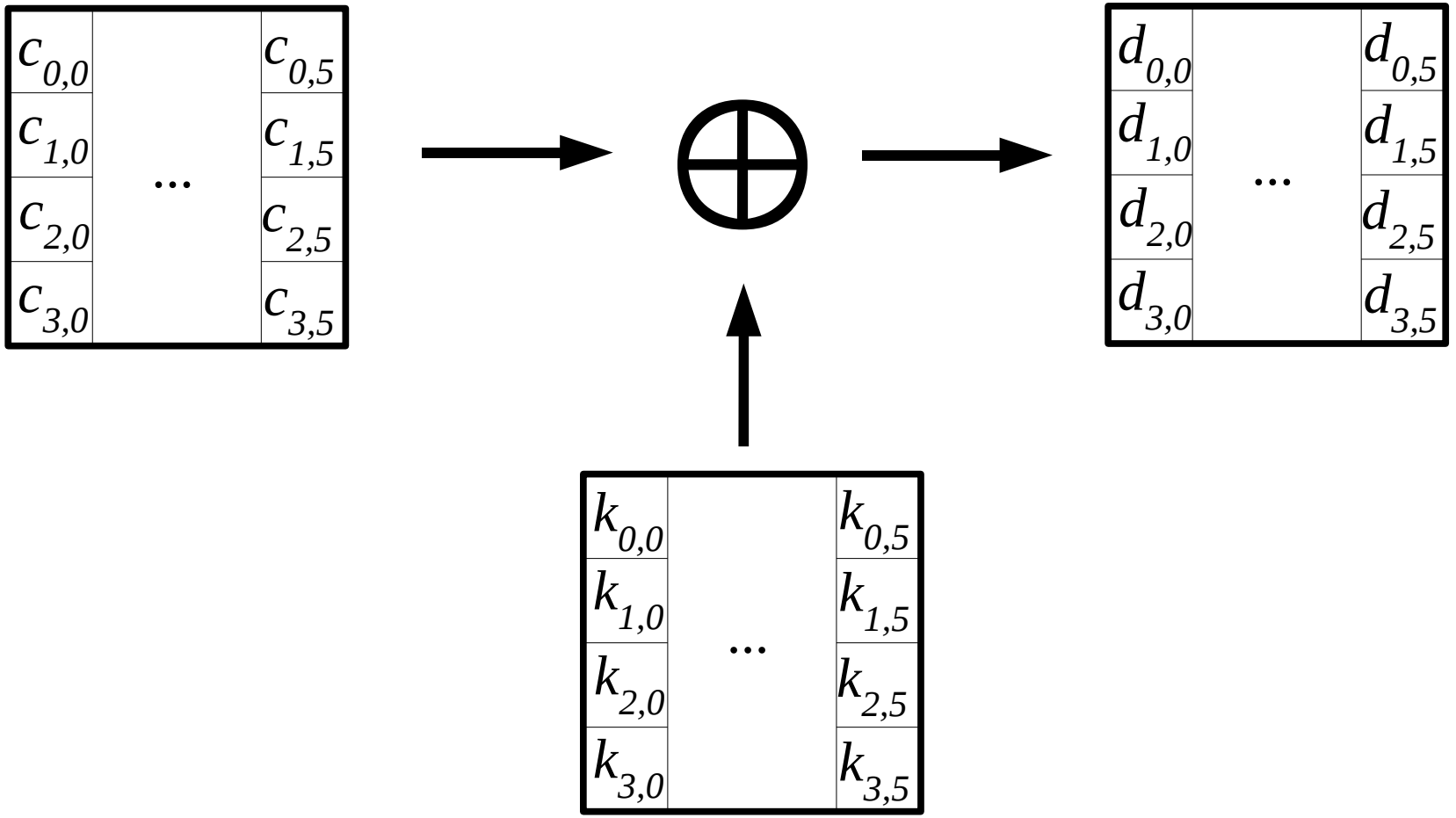
02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Let $e(x) = e_3x^3+e_2x^2+e_1x^1+e_0$, where e_3=0x03, e_2=e_1=0x01, e_0=0x02

Then $c(x) = e(x)*b(x) \bmod x^4+1$, multiplication obtained via E*b

Secret Key Systems - AES

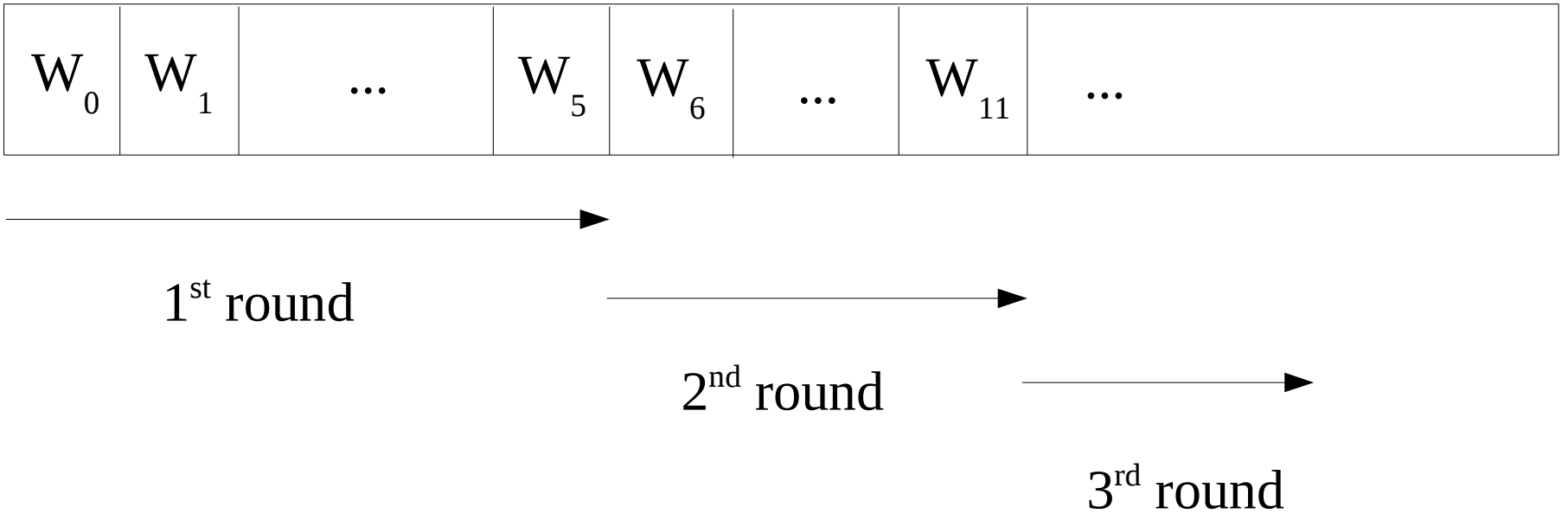
4. Round Key Addition (that is, exclusive or)



Number of round key bits = blck_lngth*(rnds+1) (e.g. 128bit, 10rnds = 1408)
Taken from expansion of cipher key
Let's forget about the expansion right now

Secret Key Systems - AES

Key Schedule example for $N_b=6$



Secret Key Systems - AES

Notes:

1. Many operations are table look ups so they are fast
2. Parallelism can be exploited
3. Key expansion only needs to be done one time until the key is changed
4. The S-box minimizes the correlation between input and output bits

Secret Key Systems - AES

Number of rounds

N_k \ N_b	4	6	8
4	10	12	14
6	12	12	14
8	14	14	14