Advanced Encryption Standard

Lars R. Knudsen

June 2014

AES - Advanced Encryption Standard

- US governmental encryption standard
- Open (world) competition announced January 97
- Blocks: 128 bits
- Keys: choice of 128-bit, 192-bit, and 256-bit keys
- October 2000: AES=Rijndael
- Standard: FIPS 197, November 2001

AES=Rijndael

- Designed by Joan Daemen and Vincent Rijmen
- Simple design, byte-oriented
- Operations: XOR and table lookup
- S-box, substitutes a byte by a byte
-

Rounds	10	12	14
Key size	128	192	256

- Focus on 128-bit key version with 10 iterations

Multiplication in GF(256) - AES

- In AES the finite field $GF(2^8)$ is determined by irreducible polynomial
$$m(x) = x^8 + x^4 + x^3 + x + 1$$

- Elements of $GF(2^8)$ are all polynomials of degree less than eight and with coefficients in $GF(2)$
- 1-to-1 correspondence between 8-bit vectors and elements in $GF(2^8)$:
  - finite field element $p(x) = \sum_{i=0}^{7} b_i x^i$.
  - 8-bit vector $v = (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0)$

Multiplication in GF(256) (cont.)

Compute $p(x)$ times $q(x)$, where $p(x) = \sum_{i=0}^{7} b_i x^i$, $q(x) = \sum_{i=0}^{7} c_i x^i$:

- Do straightforward multiplication of polynomials $p(x) \cdot q(x)$;
- Reduce result modulo $m(x)$.

Example

Compute $x^6 + x^4 + x^2 + x + 1$ times $x^7 + x + 1$

- $(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$
- $x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1 \bmod x^8+x^4+x^3+x+1 = x^7 + x^6 + 1$

Alternative representation: $57_x \times 83_x = c1_x$ (hex notation)

Multiplication by x in GF(256)

Find the product $r(x)$ of $p(x) = \sum_{i=0}^{7} b_i x^i$ and x in $GF(2^8)$:

- Compute $p(x) \cdot x = \sum_{i=0}^{7} b_i x^{i+1}$
- If $b_7 = 0$, $r(x) = p(x) \cdot x$
  If $b_7 = 1$, $r(x) = p(x) \cdot x \bmod m(x) = p(x) \cdot x + m(x)$

Example

- $(x^7 + x^6 + x^5 + x^4 + x^2) \times x = x^8 + x^7 + x^6 + x^5 + x^3$
- reduce modulo $m(x) = x^8 + x^4 + x^3 + x + 1$
- result is $x^7 + x^6 + x^5 + x^4 + x + 1$
- Hex notation: $f4_x \times 02_x = f3_x$

Multiplication by x+1 in GF(256)

Find the product $r(x)$ of $p(x) = \sum_{i=0}^{7} b_i x^i$ and $x + 1$ in $GF(2^8)$:

- Compute $(p(x) \cdot x) + p(x) = \sum_{i=0}^{7} b_i (x^i + x^{i+1})$
- If $b_7 = 0$, $r(x) = p(x) \cdot x + p(x)$
  If $b_7 = 1$,
  $r(x) = (p(x) \cdot x) + p(x) \bmod m(x) = p(x) \cdot x + p(x) + m(x)$

Example

- $(x^7 + x^6 + x^5 + x^4 + x^2) \times (x + 1) = x^8 + x^4 + x^3 + x^2$
- reduce modulo $m(x) = x^8 + x^4 + x^3 + x + 1$
- result is $x^2 + x + 1$
- Hex notation: $f4_x \times 03_x = 07_x$

AES - iterated cipher, key schedule

- Input: user selected key of 128 bits
- Output: 11 round keys $k_0, k_1, k_2, \ldots, k_{10}$
- $p = c_0$ plaintext
- $c_i = F(k_i, c_{i-1})$
- c_{10} ciphertext
- Details of key-schedule are self-study

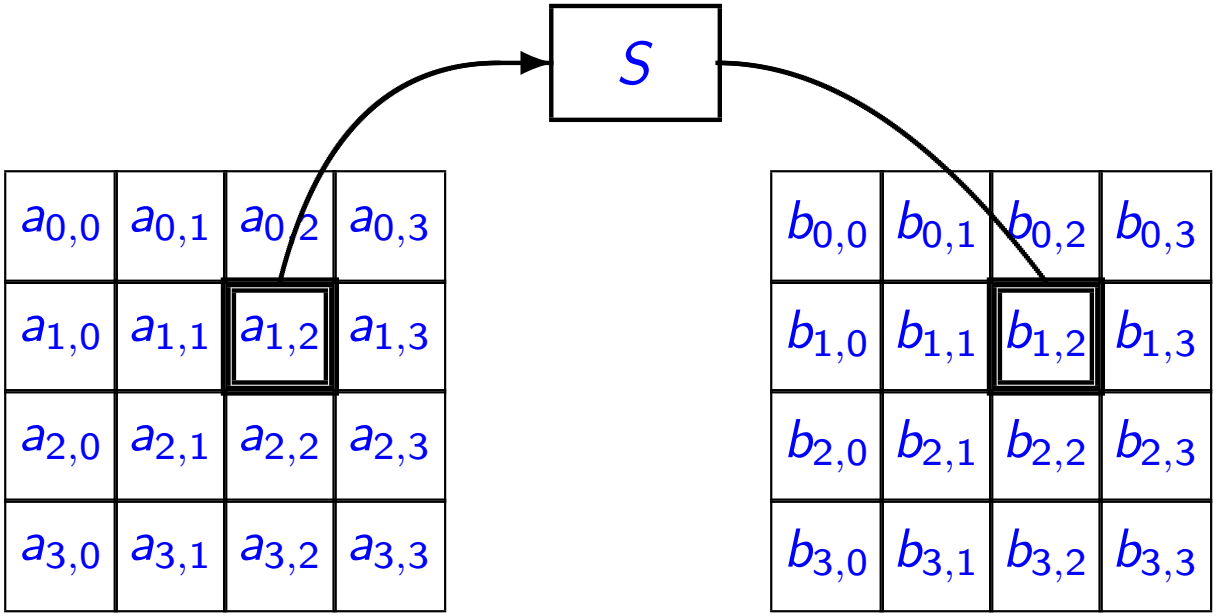
AES round tranformation

Arrange the 16 input bytes in a 4×4 matrix

Subfunctions

1. SubBytes (byte substitution via S-box)
2. ShiftRows
3. MixColumns
4. AddRoundKey

SubBytes

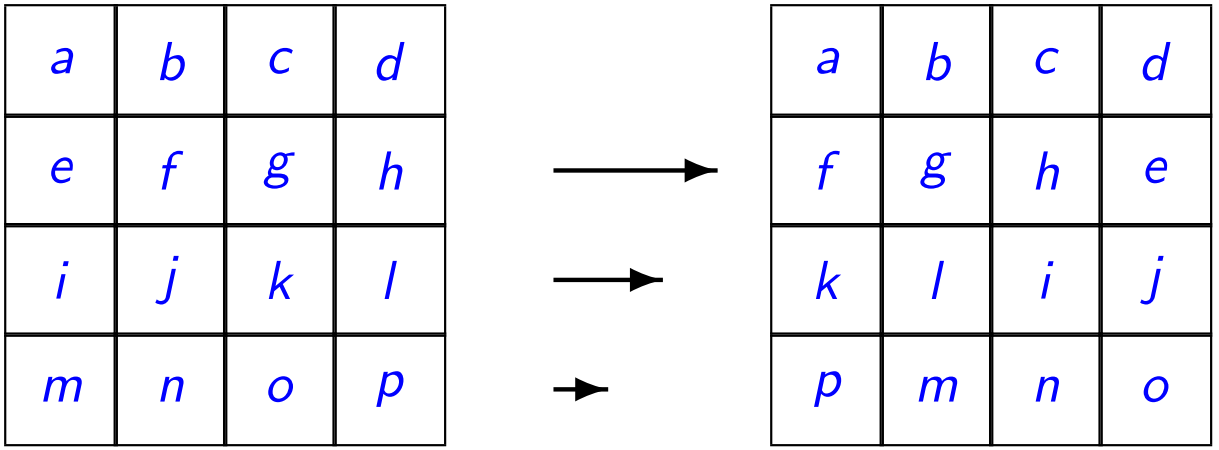


S-box

S is the S-box (invertible)

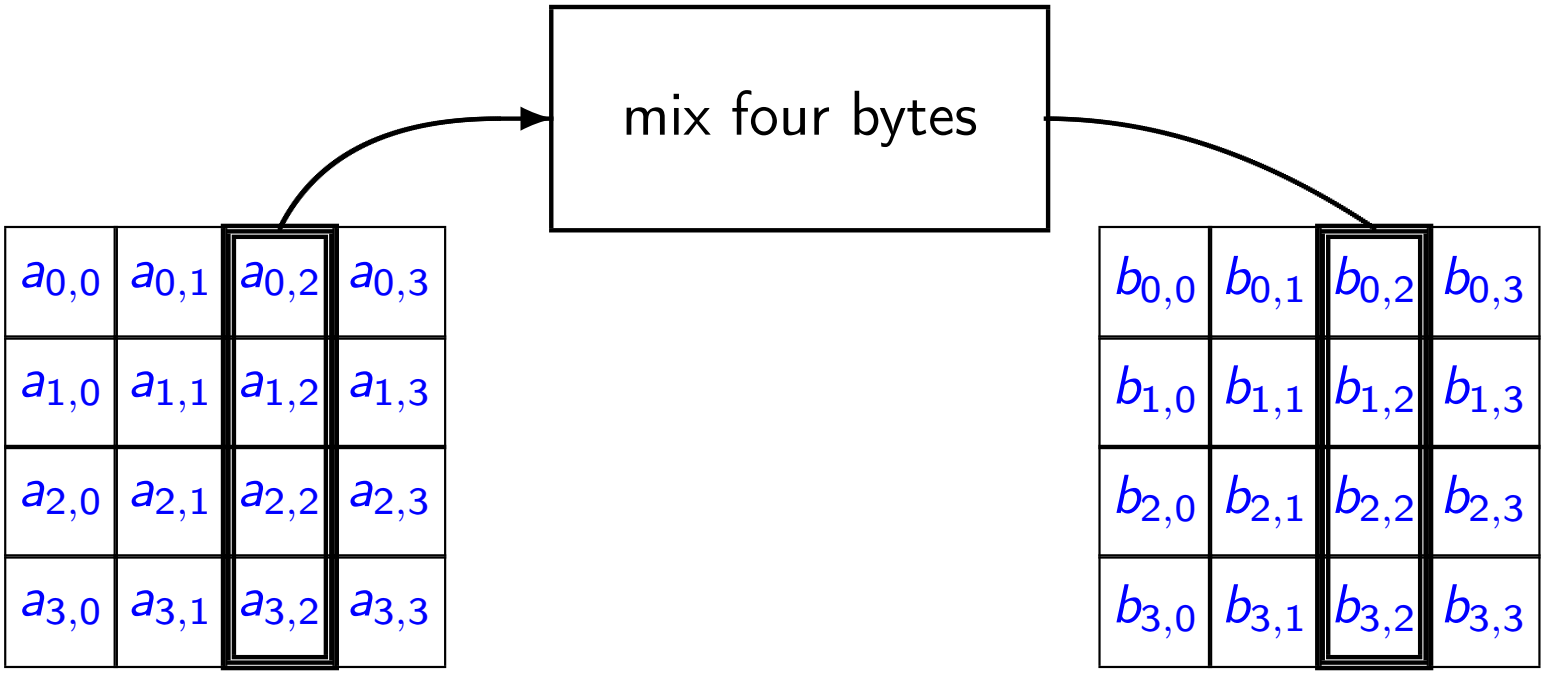
One S-box for the whole cipher (simplicity)

ShiftRows



Rows shifted over different offsets: 0,1,2, and 3

MixColumns



Each of four $b_{i,j}$ in a column depends on all four $a_{i,j}$ from same column

AddRoundKey (bit-wise XOR)

$$\begin{array}{|c|c|c|c|} \hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ \hline a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ \hline a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|} \hline k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ \hline k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ \hline k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ \hline k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \\ \hline \end{array} = \begin{array}{|c|c|c|c|} \hline b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ \hline b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ \hline b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ \hline b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \\ \hline \end{array}$$

$$b_{i,j} = a_{i,j} \oplus k_{i,j}$$

AES - 10-round version

Arrange the 16 input bytes in a 4×4 matrix

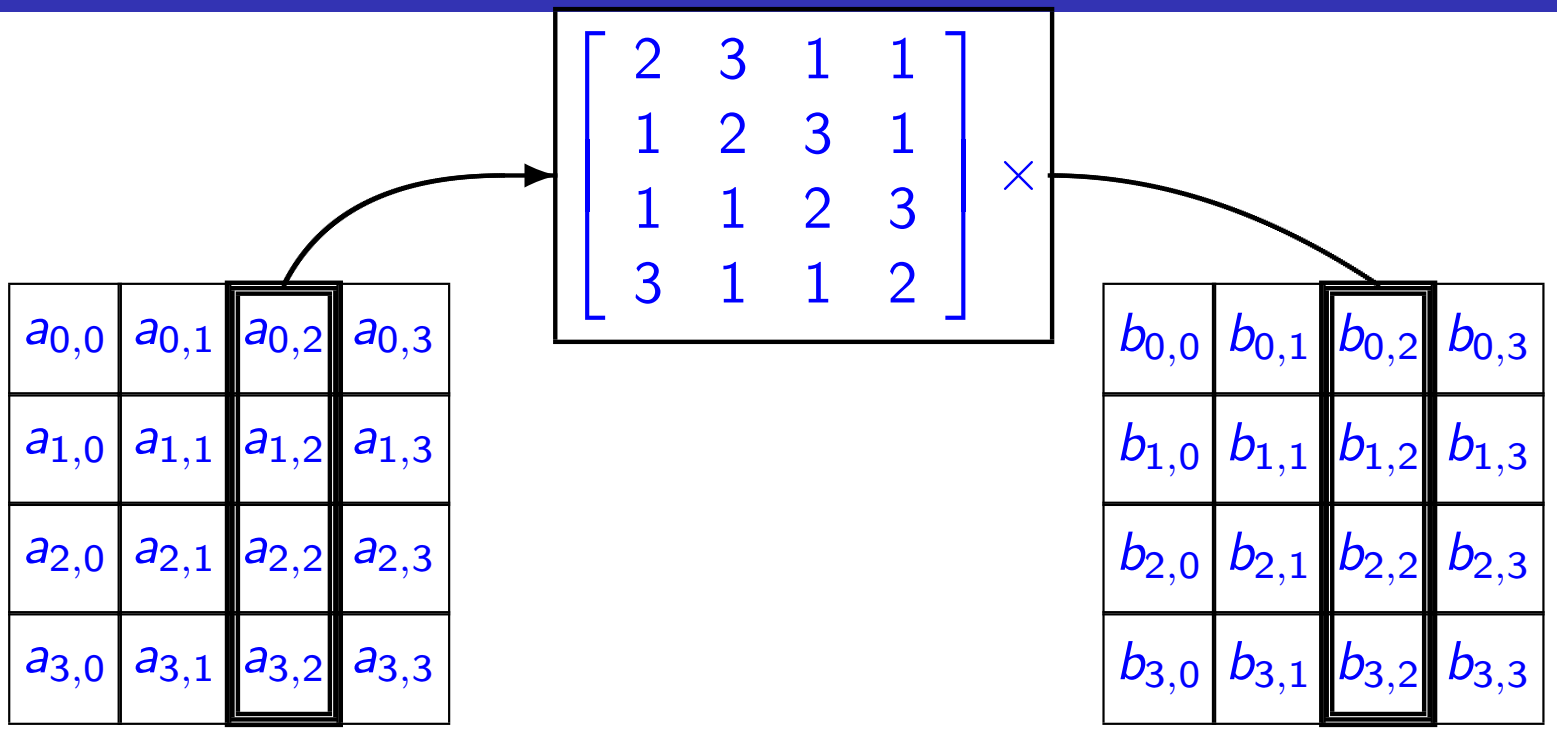
- AddRoundKey
- Do nine times
  - SubBytes (byte substitution via S-box)
  - ShiftRows
  - MixColumns
  - AddRoundKey
- SubBytes
- ShiftRows
- AddRoundKey

SubBytes

- Input a, output b, both bytes
- Let $f(x) = x^{-1}$ in $GF(2^8)/\{0\}$ and $f(0) = 0$
- Then $b = A(f(a))$, where A is affine mapping over $GF(2)$. With $t = f(a) = (t_7, t_6, \ldots, t_1, t_0)$ output is:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \\ t_6 \\ t_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

MixColumns

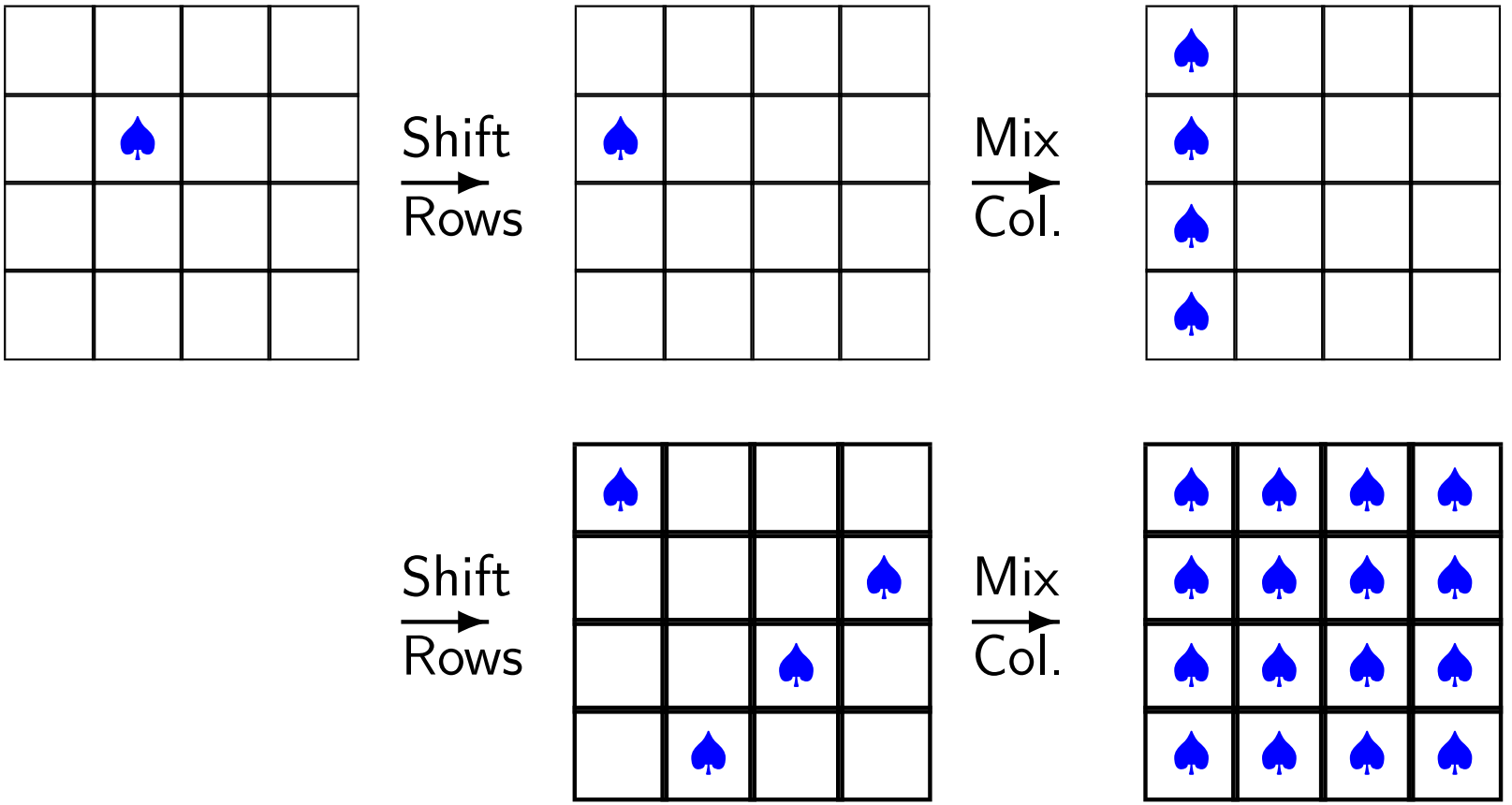


Bytes in columns are combined linearly

$$b_{0,2} = \{2\} \times a_{0,2} \ + \ \{3\} \times a_{1,2} \ + \ \{1\} \times a_{2,2} \ + \ \{1\} \times a_{3,2}$$

Multiplication is over $\mathrm{GF}(2^8)$

Diffusion in AES



Differential characteristics and active S-boxes

Consider SP-networks like AES, where a round consists of

- key addition
- S-box layer
- linear layer (linear mapping)

Definition

In a differential characteristic an S-box is *active* if the inputs to the S-box are assumed to be different.

Fact (or assumption)

The transition of differences

- *is deterministic through the key additions and linear layers.*
- *is non-deterministic through the S-box layers.*

Differential characteristics and active S-boxes (2)

Max probability

Let p_{max} be the maximum probability for a non-trivial characteristic for the S-boxes.

Active S-boxes

Let d be the minimum number of active S-boxes in an r-round characteristic.

Bound

Then p_{max}^d is an upper bound of any r-round characteristic.

AES and Wide-Trail

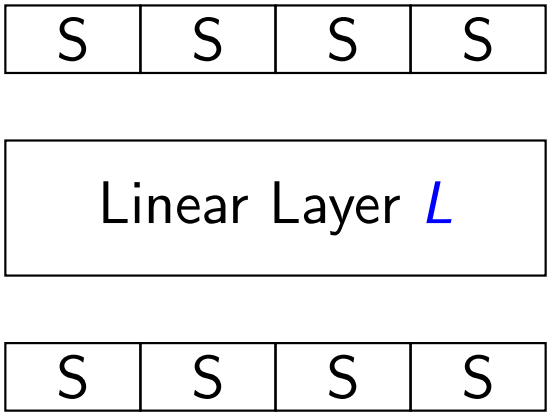
The AES design uses the wide-trail strategy:

Theorem

Any differential/linear characteristic over 4 rounds of AES has at least 25 active Sboxes.

- AES has 10 (or more) rounds
- Together with the good Sbox: More than enough.

2 Rounds



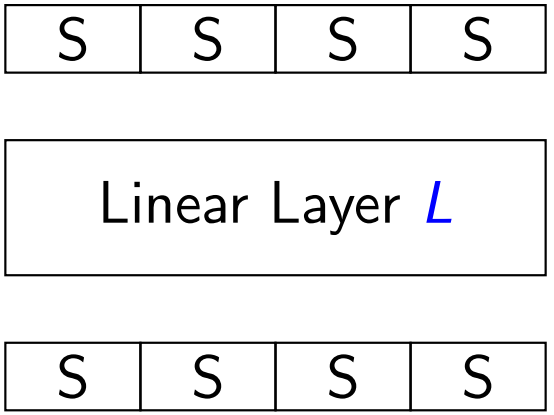
Aim

Give a bound on the number of active Sboxes in a differential characteristic.

We assume S and L are bijective.

- L linear, so $L(x \oplus y) = L(x) \oplus L(y)$.
- No further assumptions on S

2 Rounds



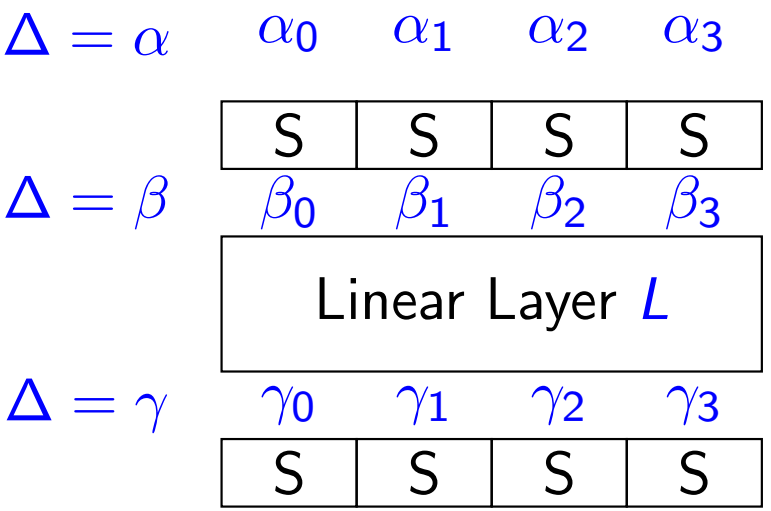
Aim

Give an lower bound on the number of active Sboxes in a differential characteristic.

Trivial bounds:

- Lower Bound for the lower bound: 2
- Upper Bound for the lower bound: $\#sboxes + 1$ (here 5).

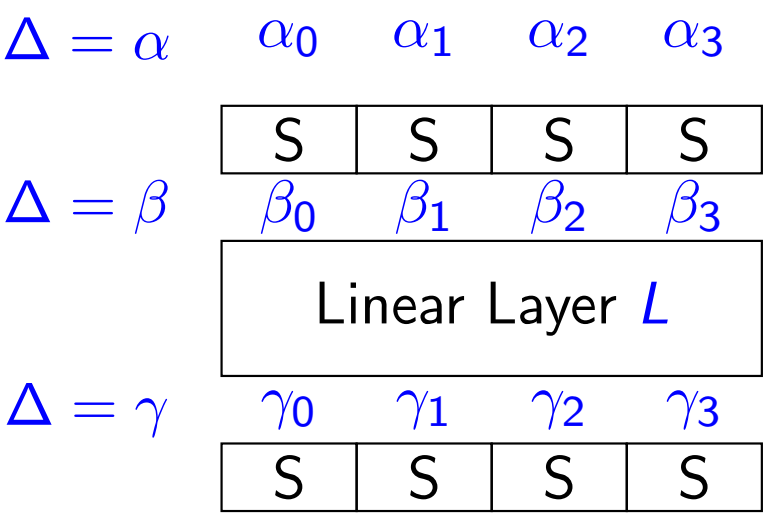
Picture with differences:



- $\gamma = L(\beta)$
- # active Sboxes is

$$|\{i \mid \alpha_i \neq 0\}| + |\{j \mid \gamma_j \neq 0\}| = |\{i \mid \beta_i \neq 0\}| + |\{j \mid \gamma_j \neq 0\}|$$

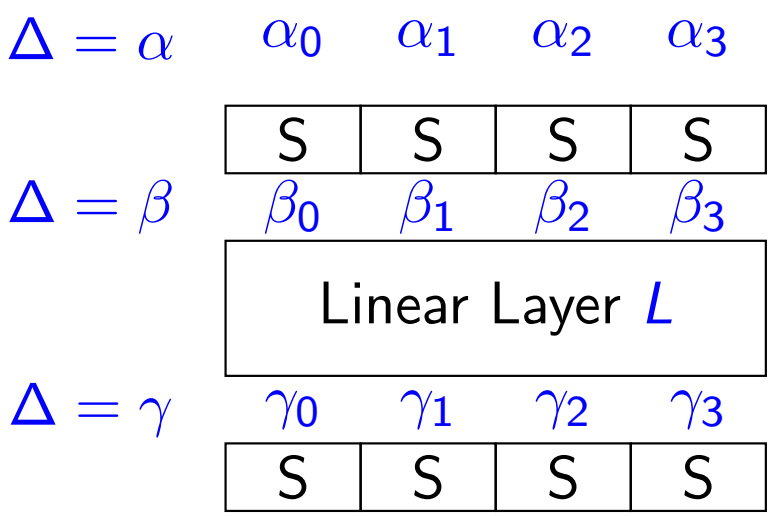
Trivial lower bound on 2 rounds



Lower bound: 2

- $\alpha \neq 0$ (at least one $\alpha_i \neq 0$).
- $\Rightarrow \beta \neq 0$ (at least one $\beta_i \neq 0$). (Sbox bijective)
- $\Rightarrow \gamma \neq 0$ (at least one $\gamma_i \neq 0$). (L is bijective)
- $\Rightarrow |\{i \mid \alpha_i \neq 0\}| + |\{j \mid \gamma_j \neq 0\}| \geq 1 + 1 = 2$

Trivial upper bound on 2 rounds



Upper bound on the lower bound: $\#sboxes + 1$ (here 5).

$$|\{i \mid \alpha_i \neq 0\}| + |\{j \mid \gamma_j \neq 0\}| \leq 1 + 4 = 5$$

Definition

The branch number of a linear transformation L is the minimum number of active words (Sboxes) in the inputs and outputs of L.

AES MixColumns - branch number

`MixColumns`: multiplication of a (4×1) $\mathrm{GF}(2^8)$-column vector by a (4×4) $\mathrm{GF}(2^8)$-matrix M given by

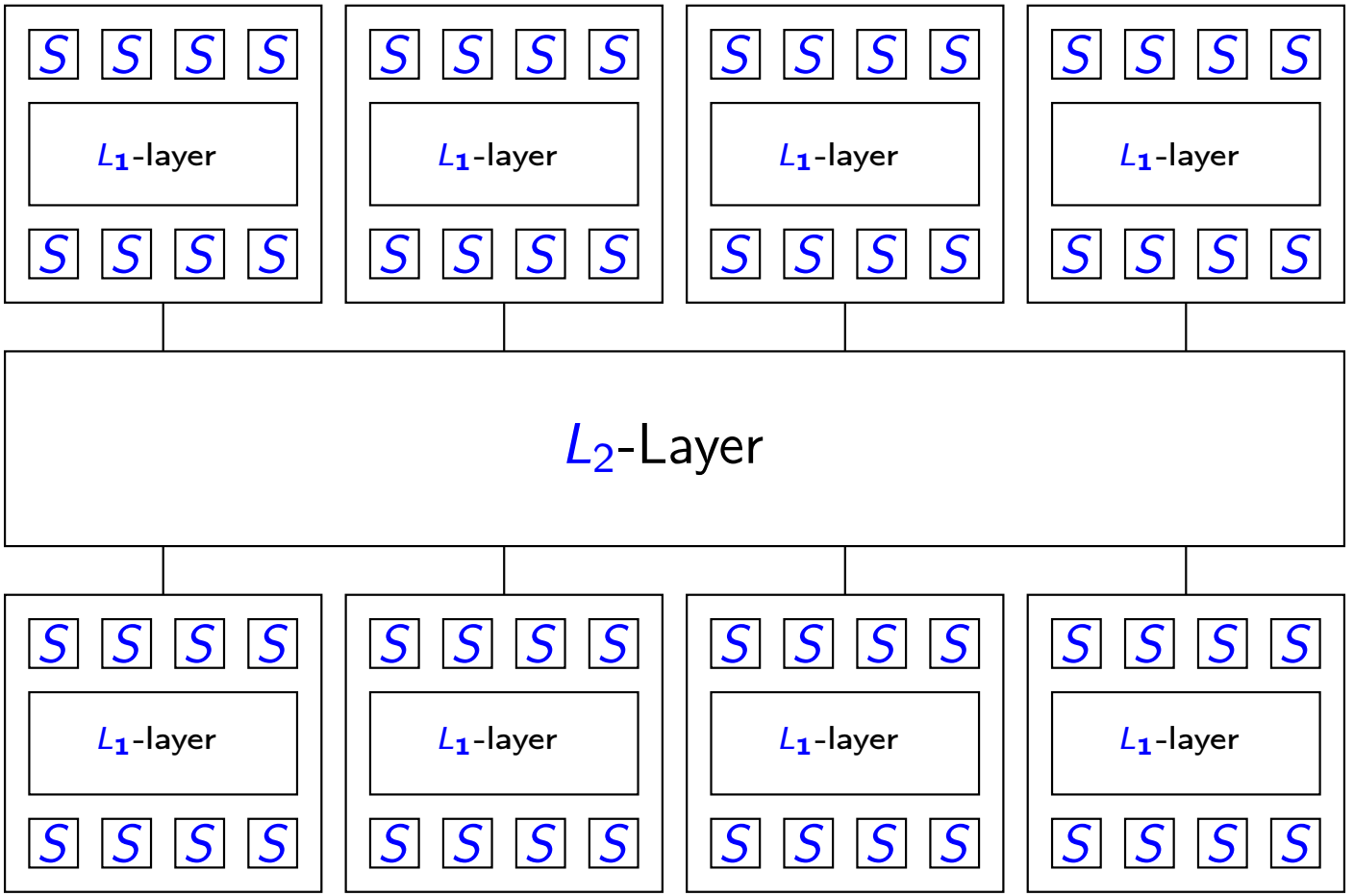
$$M = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}.$$

M derived from MDS code over $GF(2^8)$ with parameters $[8, 4, 5]$.

Fact

The branch number of `MixColumns` *is five.*

4 rounds of AES - the super box



4 rounds of AES

- Choose L_1 to ensure b_1 sboxes in each Super-Box
- Choose L_2 to ensure b_2 active Super-Boxes

Concatenation of Codes

Each characteristic over 4 rounds has at least $b_1 \cdot b_2$ active Sboxes.

For AES: $b_1 = b_2 = 5$ thus 25 active Sboxes over 4 rounds.

Bounds of probabilities of characteristics of the AES

- 25 active Sboxes over 4 rounds.
- S-box is differentially 4-uniform, so maximum probability of characteristic is

$$4/2^8 = 2^{-6}.$$

- maximum probability for characteristic over 4 rounds is 2^{-150}.
- maximum probability for characteristic over 8 rounds is 2^{-300}.

Integral cryptanalysis or the Square attack

Lars R. Knudsen

June 2014

Integral cryptanalysis

- $(G, +)$ finite abelian group, order k
- S a set of vectors in $G \times G \times \cdots \times G$
- An integral over S:

$$\sum_{v \in S} v$$

  where summation is defined by '+'
- Typically, a vector element is a plaintext/ciphertext word and a vector represents a plaintext or ciphertext

Integrals, cont.

- Let $v(i) = (v_0(i), v_1(i), \ldots, v_{n-1}(i)) \in G^n$
- Let S a set of vectors $\{v(i)\}$
- Three distinct cases where c_j and s are some known values

Case	Notation	
$v_j(i) = c_j$ for all $v(i) \in S$	$\mathcal{C}$	"constant"
$\{v_j(i) \mid v(i) \in S\} = G$	$\mathcal{A}$	"all"
$\sum_{v(i) \in S} v_j(i) = s$	$\mathcal{S}$	sum is known

- In most (all?) cases the integral over S can be determined

Useful facts

Theorem

$(G,+)$ finite abelian additive group, let $H = \{g \in G \mid g+g=0\}$. Then $s(G) = \sum_{g\in G} g = \sum_{h\in H} h$.

Example

$G = Z/mZ$, even m: $s(G) = m/2$, odd m: $s(G) = 0$.
$G = GF(2^s)$: $s(G) = 0$.

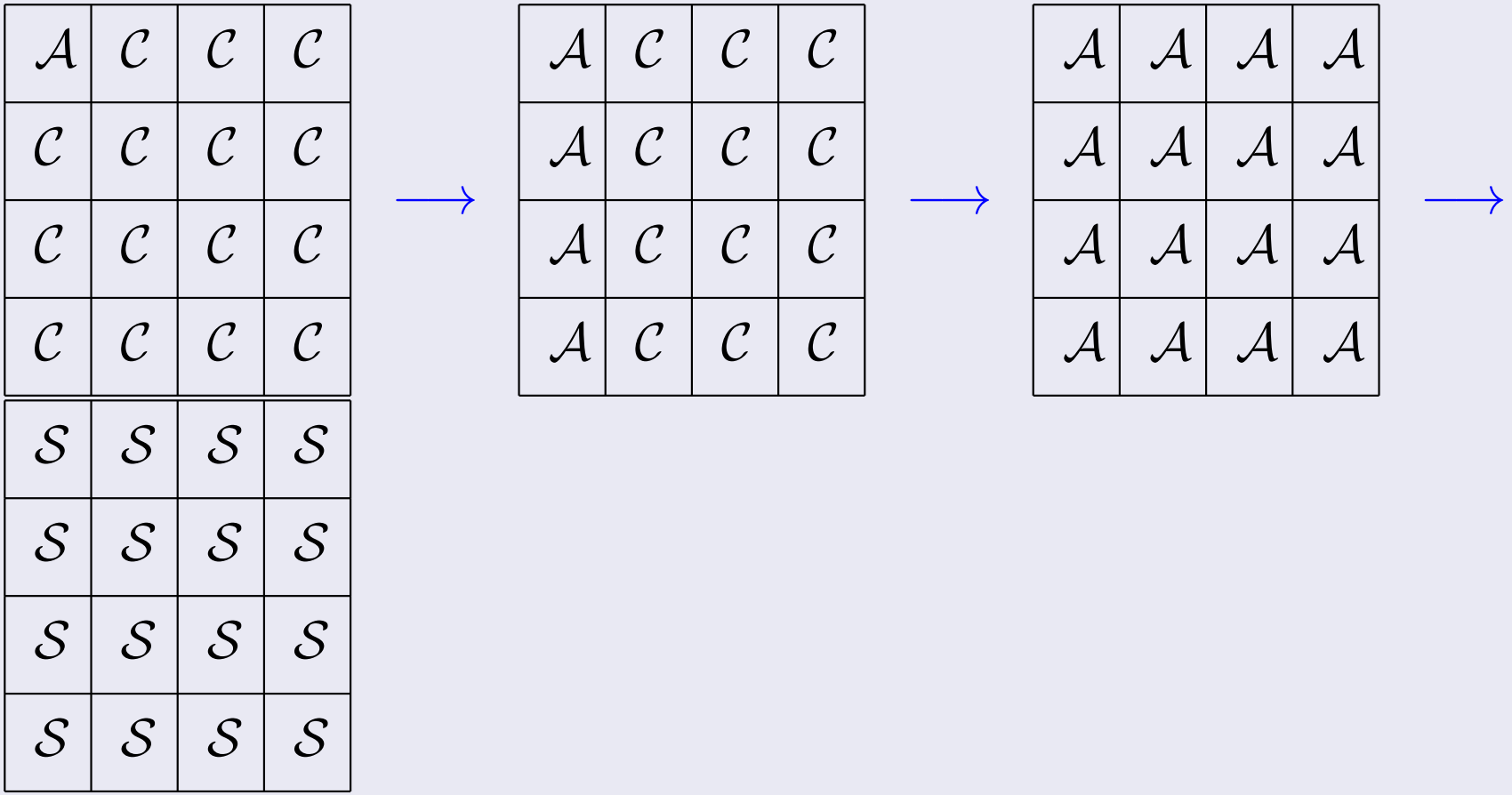
Theorem

$(G,*)$ finite abelian multiplicative group, let $H = \{g \in G \mid g*g=1\}$. Then $p(G) = \prod_{g\in G} g = \prod_{h\in H} h$.

Example

For $G = Z/pZ$ for p prime: $p(G) = p-1$.

AES - (first-order) 3-round integral, 256 texts



Here $\mathcal{S} = 0$

Attack on AES reduced to four rounds

- Use three-round integrals with 2^8 texts
- Compute backwards from ciphertexts "to $\mathcal{S}$" guessing one byte of last-round key
- Repeat for all sixteen bytes in last-round key
- Running time is approximately that of $c \times 16 \times 2^8$ encryptions for small $c > 1$

Attack on AES reduced to five rounds

- One byte after i rounds of encryption, affects only 4 bytes after $i+1$ rounds of encryption
- Use three-round fourth-order integral with 2^8 texts
- Compute backwards from ciphertexts "to $\mathcal{S}$" guessing four bytes in last-round key and one byte of second-to-last round key
- Repeat for all sets of four bytes in last-round key
- Running time is approximately that of $c_2 \times 4 \times 2^8$ encryptions for $c_2 \simeq 20$

Higher Order Integrals

Sets of vectors $\tilde{S} = S_1 \cup \cdots \cup S_s$ where each S_i forms an integral

If integral over each S_i is known, the integral over $\tilde{S}$ known

Suppose a word can take m values

- a first-order integral:
  a set of m vectors different in only in one word
- a dth-order integral:
  a set of m^d vectors different in d components, s.t. each of m^d possible values for the d-tuple occurs exactly once

Notation: $\mathcal{A}^d$

AES: four-round fourth-order integral

$\mathcal{A}^4$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
$\mathcal{C}$	$\mathcal{A}^4$	$\mathcal{C}$	$\mathcal{C}$
$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}^4$	$\mathcal{C}$
$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}^4$

$\longrightarrow$

$\mathcal{A}^4$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
$\mathcal{A}^4$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
$\mathcal{A}^4$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$
$\mathcal{A}^4$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$

$\longrightarrow$

$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$
$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$
$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$
$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$

$\longrightarrow$

$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$
$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$
$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$
$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$	$\mathcal{A}^4$

$\longrightarrow$

$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$
$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$
$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$
$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$

Attack on AES reduced to six rounds

- Use four-round fourth-order integral with 2^{32} texts
- Compute backwards from ciphertexts guessing 5 bytes of secret key
- Running time is approximately that of 2^{42} encryptions