

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.*

AES and Wide-Trail

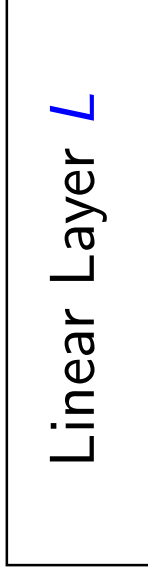
The AES design uses the wide-trail strategy:

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 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).

AES MixColumns - branch number

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

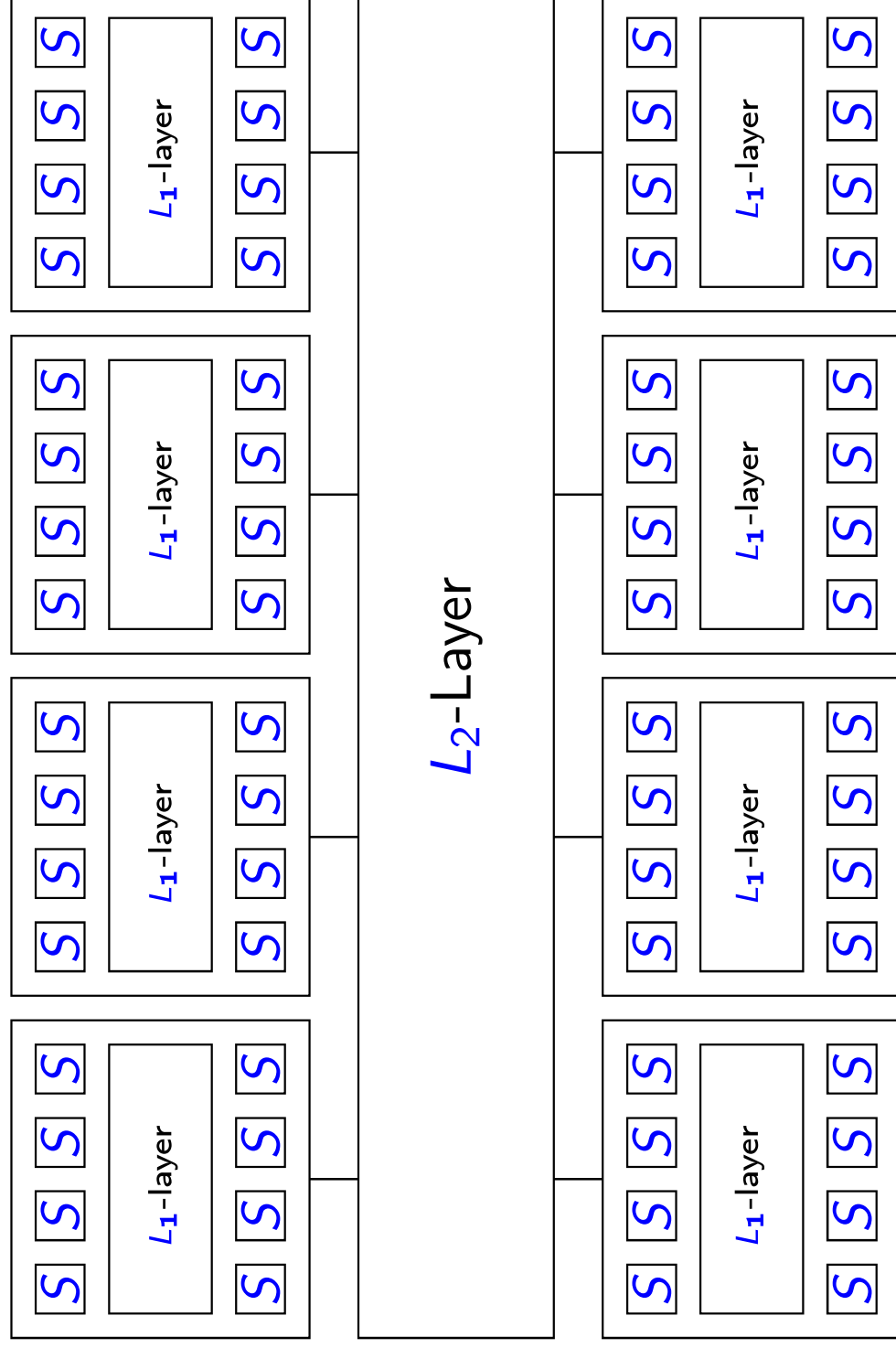
$$M = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}.$$

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} .