The Impossible Differential Attack on 5-round AES

Christophe Clavier

University of Limoges

Master 2 Cryptis

States and cells

Definition (state)

A state $(s)_{i,j}$ is a 4 x 4 matrix of bytes representing any intermediate state in an AES computation process.

Definition (cell)

For $i, j \in \{0, 1, 2, 3\}$, the cell (i, j) is simply the element at raw i, column j of a given state.

Example

	0	1	2	3
0	32	88	31	E0
1	43	5A	31	37
2	F6	30	98	07
3	A8	8D	A2	34

The content of the cell (3,1) of this state is 8D.

Active and inactive cells

Definition (active cell)

Given two states s and s', the cell (i,j) is said to be active if:

$$s_{i,j} \neq s'_{i,j}$$

Definition (inactive cell)

Given two states s and s', the cell (i,j) is said to be inactive if:

$$s_{i,j} = s'_{i,j}$$

Example

32	88	31	E0
43	5A	31	37
F6	30	98	07
A8	8D	A2	34

6F	88	31	E0
43	5A	F4	37
F6	30	98	07
A8	8D	A2	34

Cells (0,0) and (1,2) are active.

Notation: 

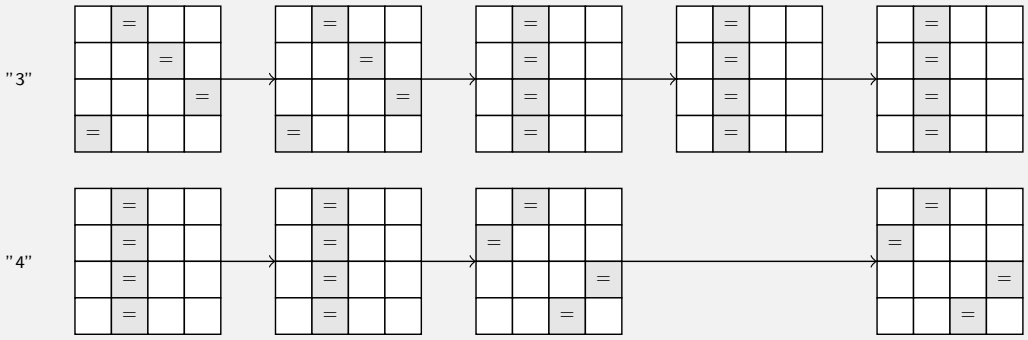
Rounds 1 and 2

Two initial states (plaintexts) having only one active cell become entirely active at the end of round 2.

Université de Limoges

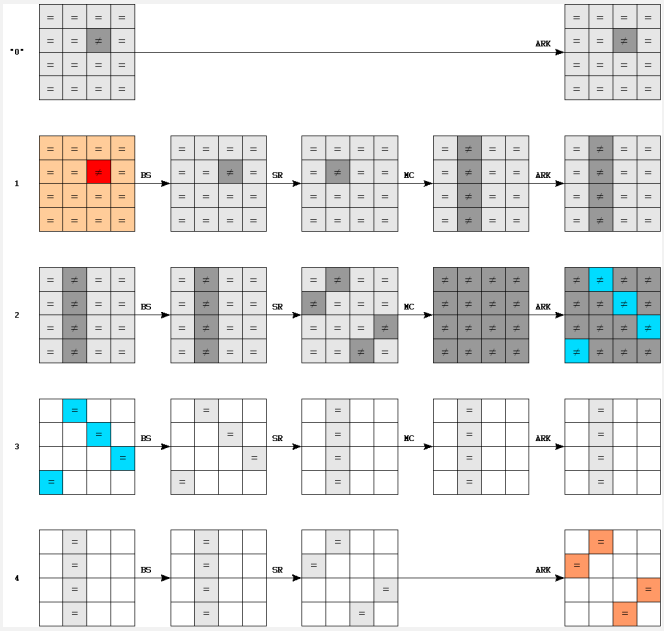
Rounds 3 and 4

If two final states (ciphertexts) are equal on some specific combination of four cells (*e.g.*, cells {(0,1),(1,0),(2,3),(3,2)}), then they are necessarily equal on some four cells at the beginning of round 3.



Other combinations are {(0,0),(1,3),(2,2),(3,1)}, {(0,2),(1,1),(2,0),(3,3)} and {(0,3),(1,2),(2,1),(3,0)}.

What is impossible



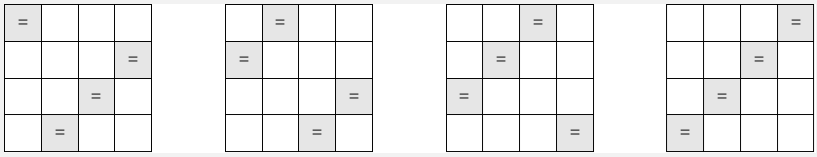
For two different inputs of an n-round AES, it is impossible to simultaneously have:

- Equality of the outputs on some specific 4-cells combination
- One and only one active cell at the beginning of round $n-3$

Principle

- A chosen message (impossible) differential attack
- One more round is added at the beginning of the 4-round impossible differential
- A set of 2^{32} chosen messages are input to a 5-round AES
  - All 2^{32} messages are equal on all but one input quadruplet where they take all possible values
- Pairs of ciphertexts showing a target output differential bring information about some part of K_0 and allow key space reduction

Four possible target output differentials:



Key observation

When a target output differential is obtain for some pair of ciphetext:

- the attacker knows that it is impossible for the two states at the beginning of round 2 (and so, at the output of MixColumns of the first round) to have one and only one active cell
- he is able to invalidate all corresponding quadruplet of K_0 which would lead to only one active cell at output of the MixColumns in the first round

Attack complexity

Exploiting about 2^{28} informative ciphertext pairs reveals the value of four K_0 bytes