The SQUARE Attack on 4-round AES

Christophe Clavier

University of Limoges

Master 2 Cryptis

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.

Definition (λ-set)

A set of 256 states $(s^{(t)})_{t=0\ldots255}$ is called a λ-set if each cell (i,j) is either *active* or *inactive* through this set of states.

Definition (active cell)

A cell (i,j) is said to be active through a set $(s^{(t)})_t$ of 256 states if:

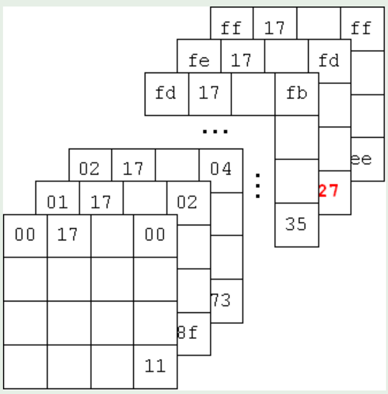
$$\{s_{i,j}^{(t)} : t = 0\ldots255\} = \{0\ldots255\}$$

Definition (inactive cell)

A cell (i,j) is said to be inactive along a set $(s^{(t)})_t$ of 256 states if there exists a constant c such that:

$$\{s_{i,j}^{(t)} : t = 0\ldots255\} = \{c\}$$

Example



Is it a λ-set ?
No !

And now ?
It may be ...

Properties of λ-sets

AddRoundKey

The image of an active (resp. inactive) cell by the `AddRoundKey` transformation is an active (resp. inactive) cell at the same position.

SubBytes

The image of an active (resp. inactive) cell by the `SubBytes` transformation is an active (resp. inactive) cell at the same position.

Properties of λ-sets

ShiftRows

The image of an active (resp. inactive) cell by the `ShiftRows` transformation is an active (resp. inactive) cell whose location has been shifted.

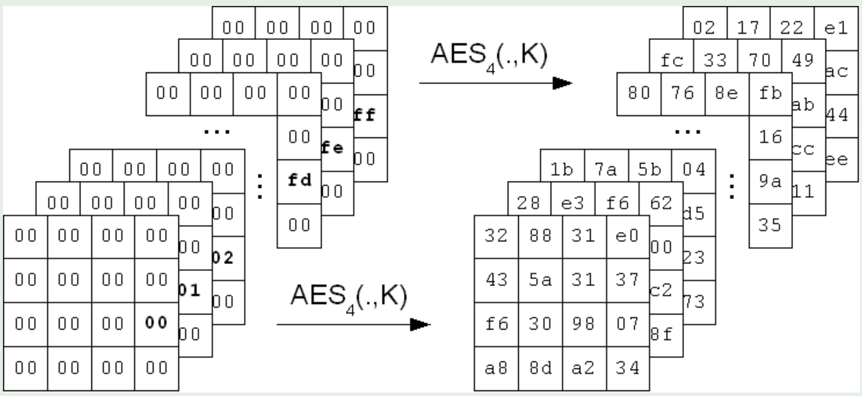
MixColumns

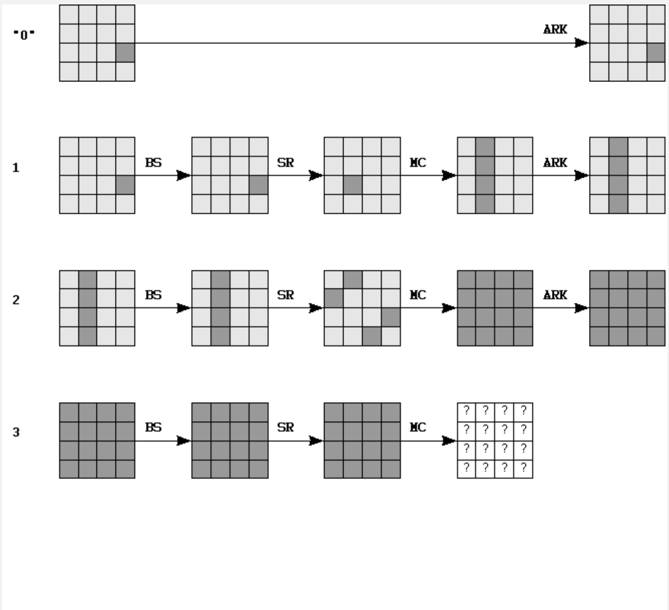
- The image of a column containing 4 inactive cells by the `MixColumns` transformation is a column containing 4 inactive cells.
- The image of a column containing 3 inactive and 1 active cells by the `MixColumns` transformation is a column containing 4 active cells.
- No similar conclusion hold in other cases.

The attack

- SQUARE is a chosen message attack.
- The attacker obtains the 256 ciphertexts corresponding to a particular λ-set of his choice.
- This λ-set is arbitrary except that it must contain one and only one active cell (and so 15 inactive ones).

Example





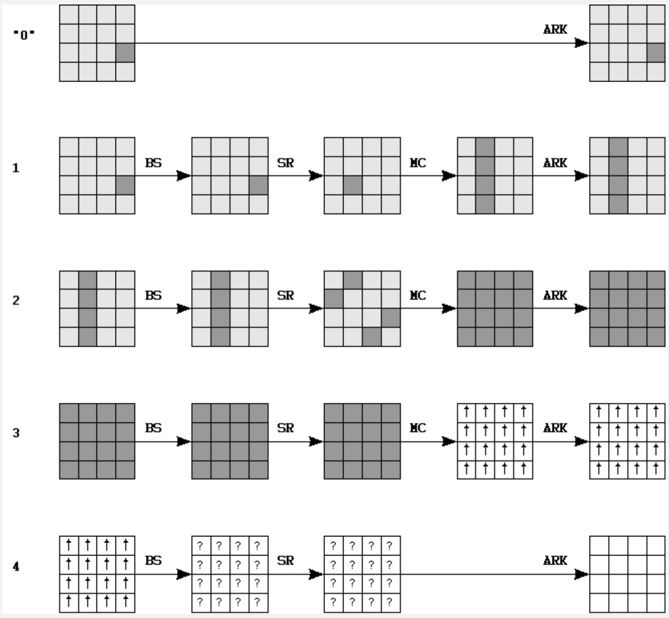
Definition (balanced cell)

A cell (i, j) is said to be balanced along a set $(s^{(t)})_t$ of 256 states if:

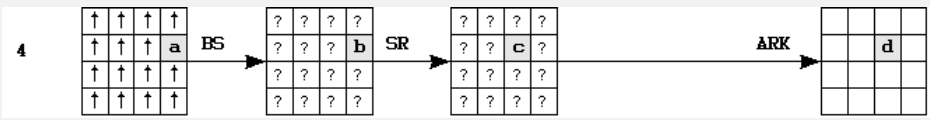
$$\bigoplus_{t=0}^{255} s_{i,j}^{(t)} = 0$$

MixColumns

- The image of a column containing 4 inactive cells by the `MixColumns` transformation is a column containing 4 inactive cells.
- The image of a column containing 3 inactive and 1 active cells by the `MixColumns` transformation is a column containing 4 active cells.
- The image of a column containing 4 balanced cells by the `MixColumns` transformation is a column containing 4 balanced cells.



- When the input of a 4-round AES is a λ-set with only one active cell, the input of the last round is made of 16 balanced cells.
- This property is exploited in order to give information about each byte of the last round key K_4.
- Knowing the output state d of the algorithm, the knowledge of only one byte $k_{l,m}$ of K_4 is enough to predict the value of one byte $a_{i,j}$ of the state a at the beginning of the last round:



$$a_{1,3} = \texttt{SubBytes}^{-1}(b_{1,3}) = \texttt{SubBytes}^{-1}(c_{1,2}) = \texttt{SubBytes}^{-1}(d_{1,2} \oplus k_{1,2})$$

- Each guess on $k_{1,2}$ is suggested if it implies the balance of the set $(a_{1,3}^{(t)})_t$.
- Beside the correct key byte value, only one false candidate remains on average.
- The whole key may be found either by exhaustive search or by intersecting product sets corresponding to different input λ-sets.