



## On subspace trails cryptanalysis

Daniel Coggia

► **To cite this version:**

Daniel Coggia. On subspace trails cryptanalysis. JC2 2018 - Journées Codage et Cryptographie, Oct 2018, Aussois, France. hal-01960306

**HAL Id: hal-01960306**

**<https://hal.inria.fr/hal-01960306>**

Submitted on 19 Dec 2018

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# On subspace trails cryptanalysis

Daniel Coggia

Inria Paris, Project Team SECRET

October 8, 2018

# Outline

## The AES and the distinguisher of [GRR17]

- The AES

- The distinguisher of Grassi, Rechberger and Rønjom

## Proof for the distinguisher

- Case of the AES

- Towards a more general lemma

- Example on another SPN: Midori

## Conclusion

## The AES and the distinguisher of [GRR17]

### The AES

The distinguisher of Grassi, Rechberger and Rønjom

Proof for the distinguisher

Conclusion

## The AES

NIST standard since 2001, SPN on **10 rounds**, **128-bit** blocks [DR02].

$$x = \begin{pmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{pmatrix} \in \mathbb{F}_{2^8}^{16}$$

$$\text{S-box} \begin{cases} \mathbb{F}_{2^8} & \rightarrow \mathbb{F}_{2^8} \\ x_i & \mapsto y_i \end{cases}$$

$$SR(y) = \begin{pmatrix} y_0 & y_4 & y_8 & y_{12} \\ y_5 & y_9 & y_{13} & y_1 \\ y_{10} & y_{14} & y_2 & y_6 \\ y_{15} & y_3 & y_7 & y_{11} \end{pmatrix}$$

ShiftRows  $SR$

$$MC(z) = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \times z$$

MixColumns  $MC$

## The AES and the distinguisher of [GRR17]

The AES

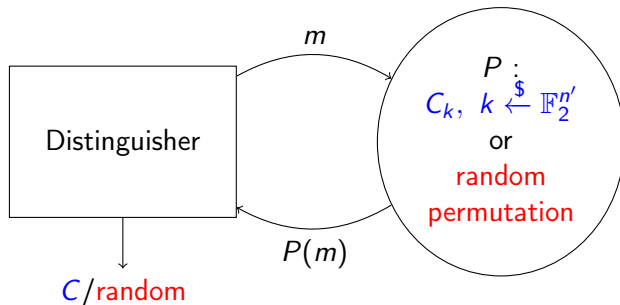
The distinguisher of Grassi, Rechberger and Rønjom

Proof for the distinguisher

Conclusion

## What is a distinguisher ?

Let  $C_k$  be a cipher with key  $k$ ,



Distinguisher  $\rightarrow$  **attack** (on more rounds).

Grassi, Rechberger and Rønjom at Eurocrypt 2017 [GRR17]

$\rightarrow C = 5$  AES rounds.

## Some definitions...

$$\mathbb{K} = \mathbb{F}_{2^8} \quad \begin{pmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{pmatrix} \in \mathcal{M}_4(\mathbb{K}) \quad x_i \in \mathbb{K}$$

$$\begin{pmatrix} x_0 & 0 & 0 & 0 \\ x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{C}_0$$

Columns

$$\mathcal{C}_i = \text{vect}_{\mathbb{K}}(e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i})$$

$$\begin{pmatrix} 0 & x_0 & 0 & y_0 \\ 0 & x_1 & 0 & y_1 \\ 0 & x_2 & 0 & y_2 \\ 0 & x_3 & 0 & y_3 \end{pmatrix} \in \mathcal{C}_{\{1,3\}}$$

 $I \subseteq \llbracket 0, 3 \rrbracket :$ 

$$\mathcal{C}_I = \bigoplus_{i \in I} \mathcal{C}_i.$$



$$\begin{pmatrix} x_0 & 0 & 0 & 0 \\ 0 & x_1 & 0 & 0 \\ 0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & x_3 \end{pmatrix} \in \mathcal{D}_0,$$

Diagonals:  
 $\mathcal{D}_i = SR^{-1}(C_i)$

$$\begin{pmatrix} x_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_1 \\ 0 & 0 & x_2 & 0 \\ 0 & x_3 & 0 & 0 \end{pmatrix} \in \mathcal{ID}_0,$$

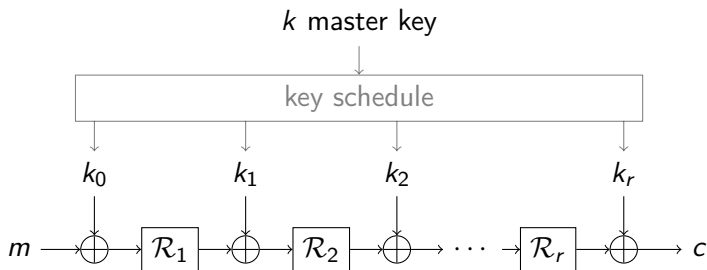
Anti-diagonals:  
 $\mathcal{ID}_i = SR(C_i)$

$$\begin{pmatrix} 2 \cdot x_0 & x_1 & x_2 & 3 \cdot x_3 \\ x_0 & x_1 & 3 \cdot x_2 & 2 \cdot x_3 \\ x_0 & 3 \cdot x_1 & 2 \cdot x_2 & x_3 \\ 3 \cdot x_0 & 2 \cdot x_1 & x_2 & x_3 \end{pmatrix} \in \mathcal{M}_0.$$

Mixed:  
 $\mathcal{M}_i = MC(\mathcal{ID}_i)$

$$\mathcal{D}_i \xrightarrow{S} \mathcal{D}_i \xrightarrow{SR} \mathcal{C}_i \xrightarrow{MC} \mathcal{C}_i \xrightarrow{S} \mathcal{C}_i \xrightarrow{SR} \mathcal{ID}_i \xrightarrow{MC} \mathcal{M}_i$$

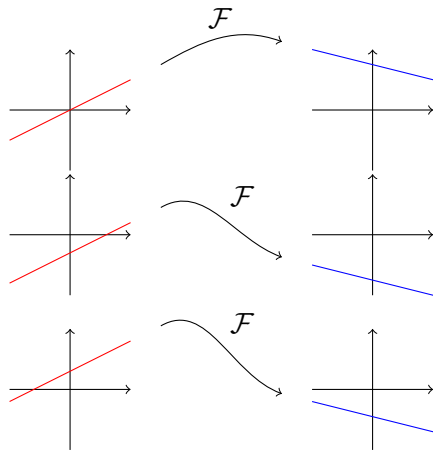
# The AES is a key-alternating blockcipher



## Subspace trails

### Definition ([LTW18])

We have  $U \xrightarrow{\mathcal{F}} V$  if  $\forall a \in \mathbb{K}^N, \exists b \in \mathbb{K}^N : \mathcal{F}(U + a) \subseteq V + b$ .



### Examples:

- ▶  $\{0\} \xrightarrow{\mathcal{F}} \{0\}$
- ▶  $U \xrightarrow{\mathcal{F}} \mathbb{K}^N$
- ▶  $\mathcal{D}_I \xrightarrow{\mathcal{R}} \mathcal{C}_I$
- ▶  $\mathcal{C}_I \xrightarrow{\mathcal{R}} \mathcal{M}_I$

$$\mathcal{D}_0 \stackrel{\mathcal{R}}{\Rightarrow} \mathcal{C}_0$$

$$\forall a, \forall x,$$

$$\begin{array}{c}
 \begin{pmatrix} x_0 & 0 & 0 & 0 \\ 0 & x_1 & 0 & 0 \\ 0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & x_3 \end{pmatrix} \xrightarrow{+a} \begin{pmatrix} x_0 + a_0 & * & * & * \\ * & x_1 + a_1 & * & * \\ * & * & x_2 + a_2 & * \\ * & * & * & x_3 + a_3 \end{pmatrix} \\
 \\
 \begin{matrix} \xrightarrow{S} \\ \xrightarrow{SR} \end{matrix} \begin{pmatrix} y_0 & * & * & * \\ * & y_1 & * & * \\ * & * & y_2 & * \\ * & * & * & y_3 \end{pmatrix} \begin{pmatrix} y_0 & * & * & * \\ y_1 & * & * & * \\ y_2 & * & * & * \\ y_3 & * & * & * \end{pmatrix} \\
 \\
 \xrightarrow{MC} \begin{pmatrix} \vdots & * & * & * \\ \vdots & * & * & * \\ MC(y) & * & * & * \\ \vdots & * & * & * \end{pmatrix}
 \end{array}$$

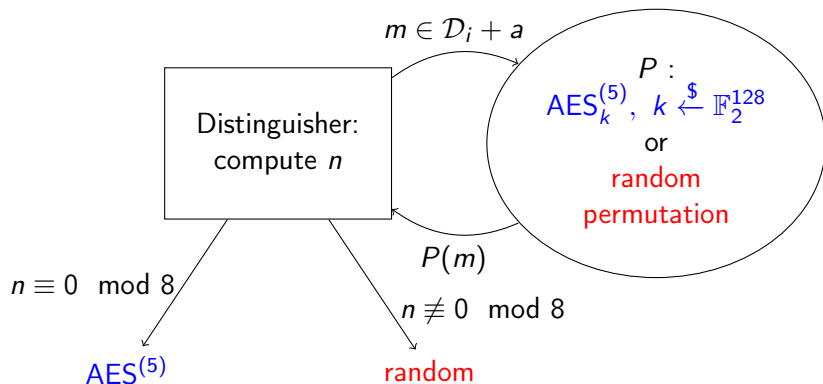
# The distinguisher

## Theorem ([GRR17])

Let  $a \in \mathcal{M}_4(\mathbb{K})$ ,  $i \in \llbracket 0, 3 \rrbracket$ ,  $J \subseteq \llbracket 0, 3 \rrbracket$ . We define

$$n = \#\{ \{p^0, p^1\} \in \mathcal{P}^2(\mathcal{D}_i + a) \mid \mathcal{R}^5(p^0) + \mathcal{R}^5(p^1) \in \mathcal{M}_J \}.$$

Then  $n \equiv 0 \pmod 8$ .



The AES and the distinguisher of [GRR17]

Proof for the distinguisher

Case of the AES

Towards a more general lemma

Example on another SPN: Midori

Conclusion

## A key lemma

## Lemma ([GRR17])

Let  $a \in \mathcal{M}_4(\mathbb{K})$ ,  $I \subset \llbracket 0, 3 \rrbracket$ ,  $J \subset \llbracket 0, 3 \rrbracket$ . We define

$$n = \#\{ \{p^0, p^1\} \in \mathcal{P}^2(\mathcal{M}_I + a) \mid \mathcal{R}(p^0) + \mathcal{R}(p^1) \in \mathcal{D}_J \}.$$

Then  $n \equiv 0 \pmod{8}$ .

$$\begin{array}{ccccccc}
 & & \underbrace{2} & & \underbrace{1} & & \underbrace{2} \\
 & & \mathcal{R} & & \mathcal{R} & & \mathcal{R} \\
 \mathcal{D}_I & \Rightarrow & \mathcal{C}_I & \Rightarrow & \mathcal{M}_I & \xrightarrow{\text{Lemma } \mathcal{R}} & \mathcal{D}_J & \Rightarrow & \mathcal{C}_J & \Rightarrow & \mathcal{M}_J
 \end{array}$$

# Proof

## In the original paper [GRR17]:

**First case.** First, we consider the case in which three variables are set. Without loss of generality we assume for example that  $x = y^2, x' = x', w = w'$  and  $a = a'$  (the other cases are analogous). In other words, we suppose that the two  $y^2$  and  $y'^2$  belong to the same set of  $M_{2^k} \times C_{2^k}$ , where  $a \in (M_{2^k} \times C_{2^k})$ .

Since  $M_{2^k} \times C_{2^k}$  is closed, it follows that  $x^2 y^2 y'^2 \in C_{2^k}$ , then  $Ry^2 \circ Ry^2 \circ Ry^2 \circ Ry^2 \circ Ry^2 \in \{0\}$  for each  $J$  and  $J'$  with  $|J| \geq 2$  and  $|J'| \geq 2$ . In other words, the given hyperplane for this case, it is not possible that the two bytes belong to the same set of a diagonal group  $D_J$  for each  $J$ . It also can be proved.

For completeness, it is also possible to show the same result in a different way. By definition,  $Ry^2 \circ Ry^2 \circ D_J$  for a certain  $J$  with  $|J| \geq 2$  and  $a \in M_{2^k} \times C_{2^k}$  is  $\{0\}$  for each  $x, x', y, y', z, z', w, w'$ . In fact, the four bytes of the diagonal group  $D_J$  are equal to zero, when the indices are taken with  $a$  and  $J$  in  $\{0, 1, 2, 3\}$ . As we are going to show, that is not the only way of that this case and since the branch number of the MixColumns operation is 5, it follows that  $Ry^2 \circ Ry^2 \circ D_J$  for the  $J$  with  $|J| \geq 2$ . In other words  $Ry^2 \circ Ry^2 \circ D_J$  for  $|J| \geq 2$  and only if  $a = a'$ , that is  $y^2 = y'^2$ .

In more details, by simple composition the first column (and hence for other ones) of  $SBox \circ SBox^{-1} \circ SBox \circ SBox^{-1}$  obtained by  $(SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1})$  is equal to

$$(SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) = \begin{bmatrix} SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a') \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

After the MixColumns operation (note:  $Ry^2 \circ Ry^2 \circ D_J \circ Ry^2 \circ Ry^2 \circ SBox^{-1} \circ SBox^{-1} \circ SBox \circ SBox^{-1} \circ SBox \circ SBox^{-1} \circ SBox \circ SBox^{-1} \circ SBox \circ SBox^{-1} \circ SBox \circ SBox^{-1}$ ), since a one input byte  $0$  is different from zero, it follows that at least four output bytes must be different from zero, that is all the output bytes are different from zero. This clearly implies that it is not possible that  $Ry^2 \circ Ry^2 \circ D_J$  for  $|J| \geq 2$ .

**Second case.** Similarly, we consider the case in which two variables are set, that is, for example, we assume for example that  $x = x'$  and  $w = w'$ , while  $y = y', y' = y'$  (the other cases are analogous). Thus, we suppose that the two  $y$  and  $y'$  belong to the same set of  $M_{2^k} \times C_{2^k}$ , where  $a \in (M_{2^k} \times C_{2^k})$ .

Since  $M_{2^k} \times C_{2^k}$  is closed, it follows that  $x^2 y^2 y'^2 \in C_{2^k}$ , then  $Ry^2 \circ Ry^2 \circ Ry^2 \circ Ry^2 \circ Ry^2 \in \{0\}$  for each  $J$  and  $J'$  with  $|J| \geq 2$  and  $|J'| \geq 2$ . In other words, the given hyperplane for this case, it is not possible that the two bytes belong to the same set of a diagonal group  $D_J$  for each  $J$ . It also can be proved.

For completeness, it is also possible to show the same result in a different way. By definition,  $Ry^2 \circ Ry^2 \circ D_J$  for a certain  $J$  with  $|J| \geq 2$  and  $a \in M_{2^k} \times C_{2^k}$  is  $\{0\}$  for each  $x, x', y, y', z, z', w, w'$ . In fact, the four bytes of the diagonal group  $D_J$  are equal to zero, when the indices are taken with  $a$  and  $J$  in  $\{0, 1, 2, 3\}$ . As we are going to show, that is not the only way of that this case and since the branch number of the MixColumns operation is 5, it follows that  $Ry^2 \circ Ry^2 \circ D_J$  for the  $J$  with  $|J| \geq 2$ . In other words  $Ry^2 \circ Ry^2 \circ D_J$  for  $|J| \geq 2$  and only if  $a = a'$ , that is  $y = y'$ .

This implies that the two-revision  $y^2$  (generated by  $(x, y^2)$ ) and  $y'^2$  (generated by  $(x', y'^2)$ )

$$y^2 = x \begin{bmatrix} x' & y' & 0 & 0 \\ x' & y' & 0 & 0 \\ x' & y' & 0 & 0 \\ x' & y' & 0 & 0 \end{bmatrix}, \quad y'^2 = x' \begin{bmatrix} x & y & 0 & 0 \\ x & y & 0 & 0 \\ x & y & 0 & 0 \\ x & y & 0 & 0 \end{bmatrix}$$

belong to the same set of  $D_J$  after one round. To prove this fact, it is sufficient to compute  $Ry^2 \circ Ry^2 \circ D_J$  and  $Ry'^2 \circ Ry'^2 \circ D_J$ , and to prove that they are equal.

$$Ry^2 \circ Ry^2 \circ D_J = Ry'^2 \circ Ry'^2 \circ D_J$$

Since  $Ry^2 \circ Ry^2 \circ D_J \in D_J$ , it also follows that  $Ry'^2 \circ Ry'^2 \circ D_J$  is partitioned by simple composition the first column of  $Ry^2 \circ Ry^2 \circ D_J$  is given by:

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,0} = x \cdot (SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a'_{0,0}))$$

$$= x \cdot (SBox(2 \circ x_{0,0}) \circ SBox(2 \circ x'_{0,0}))$$

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,1} = x \cdot (SBox(2 \circ x + a_{1,0}) \circ SBox(2 \circ x' + a'_{1,0}))$$

$$= x \cdot (SBox(2 \circ x_{1,0}) \circ SBox(2 \circ x'_{1,0}))$$

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,2} = x \cdot (SBox(2 \circ x + a_{2,0}) \circ SBox(2 \circ x' + a'_{2,0}))$$

$$= x \cdot (SBox(2 \circ x_{2,0}) \circ SBox(2 \circ x'_{2,0}))$$

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,3} = x \cdot (SBox(2 \circ x + a_{3,0}) \circ SBox(2 \circ x' + a'_{3,0}))$$

$$= x \cdot (SBox(2 \circ x_{3,0}) \circ SBox(2 \circ x'_{3,0}))$$

The two definitions of  $y^2$  and  $y'^2$  are defined equivalently that  $(Ry^2 \circ Ry^2 \circ D_J)_{1,0}$ ,  $(Ry'^2 \circ Ry'^2 \circ D_J)_{1,0}$ . The same holds for the other columns. Note that the entries of the two-revision  $y^2$  and  $y'^2$  is influenced by the fact that we are working in the entire case of  $D_J$ . This implies that the number of collisions must be that in a multiple of 2.

Question: given  $y^2 \circ D_J$  for  $|J| \geq 2$ , how again becomes the branch number of the MixColumns operation. In fact, indeed, composition  $(SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1})$  and analyze the first column (the others are analogous).

$$(SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) = \begin{bmatrix} SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a') \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

After the MixColumns operation (note:  $Ry^2 \circ Ry^2 \circ D_J \circ Ry^2 \circ Ry^2 \circ SBox^{-1} \circ SBox^{-1} \circ SBox \circ SBox^{-1} \circ SBox \circ SBox^{-1} \circ SBox \circ SBox^{-1} \circ SBox \circ SBox^{-1}$ ), since a one input byte  $0$  is different from zero, it follows that at least four output bytes must be different from zero, that is all the output bytes are different from zero. This clearly implies that it is not possible that  $Ry^2 \circ Ry^2 \circ D_J$  for  $|J| \geq 2$ .

Note that  $SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a')$  and  $SBox(2 \circ x + a_{1,0}) \circ SBox(2 \circ x' + a')$  are equal only if  $x = x'$  and  $a = a'$ , which can never happen by hypothesis.

at least three output bytes must be different from zero, or at most one output byte could be equal to zero (similar for the other columns). In other words, it is possible that  $y^2$  and  $y'^2$  must each that  $Ry^2 \circ Ry^2 \circ D_J \in D_J$  for  $|J| \geq 2$ . Moreover, this also implies that it is not possible that two or more output bytes in the same column are equal to zero, or in other words that  $Ry^2 \circ Ry^2 \circ D_J \in D_J$  for  $|J| \geq 2$  with the previous condition.

Moreover, when that  $Ry^2 \circ Ry^2 \circ D_J \in D_J$  for  $|J| \geq 2$  and only if  $a = a'$  (the other cases are analogous). Thus, we suppose that the two  $y$  and  $y'$  belong to the same set of  $M_{2^k} \times C_{2^k}$ , where  $a \in (M_{2^k} \times C_{2^k})$ .

Since  $M_{2^k} \times C_{2^k}$  is closed, it follows that  $x^2 y^2 y'^2 \in C_{2^k}$ , then  $Ry^2 \circ Ry^2 \circ Ry^2 \circ Ry^2 \circ Ry^2 \in \{0\}$  for each  $J$  and  $J'$  with  $|J| \geq 2$  and  $|J'| \geq 2$ . In other words, the given hyperplane for this case, it is not possible that the two bytes belong to the same set of a diagonal group  $D_J$  for each  $J$ . It also can be proved.

For completeness, it is also possible to show the same result in a different way. By definition,  $Ry^2 \circ Ry^2 \circ D_J$  for a certain  $J$  with  $|J| \geq 2$  and  $a \in M_{2^k} \times C_{2^k}$  is  $\{0\}$  for each  $x, x', y, y', z, z', w, w'$ . In fact, the four bytes of the diagonal group  $D_J$  are equal to zero, when the indices are taken with  $a$  and  $J$  in  $\{0, 1, 2, 3\}$ . As we are going to show, that is not the only way of that this case and since the branch number of the MixColumns operation is 5, it follows that  $Ry^2 \circ Ry^2 \circ D_J$  for the  $J$  with  $|J| \geq 2$ . In other words  $Ry^2 \circ Ry^2 \circ D_J$  for  $|J| \geq 2$  and only if  $a = a'$ , that is  $y = y'$ .

This implies that the two-revision  $y^2$  (generated by  $(x, y^2)$ ) and  $y'^2$  (generated by  $(x', y'^2)$ )

$$y^2 = x \begin{bmatrix} x' & y' & 0 & 0 \\ x' & y' & 0 & 0 \\ x' & y' & 0 & 0 \\ x' & y' & 0 & 0 \end{bmatrix}, \quad y'^2 = x' \begin{bmatrix} x & y & 0 & 0 \\ x & y & 0 & 0 \\ x & y & 0 & 0 \\ x & y & 0 & 0 \end{bmatrix}$$

belong to the same set of  $D_J$  after one round. To prove this fact, it is sufficient to compute  $Ry^2 \circ Ry^2 \circ D_J$  and  $Ry'^2 \circ Ry'^2 \circ D_J$ , and to prove that they are equal.

$$Ry^2 \circ Ry^2 \circ D_J = Ry'^2 \circ Ry'^2 \circ D_J$$

Since  $Ry^2 \circ Ry^2 \circ D_J \in D_J$ , it also follows that  $Ry'^2 \circ Ry'^2 \circ D_J$  is partitioned by simple composition the first column of  $Ry^2 \circ Ry^2 \circ D_J$  is given by:

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,0} = x \cdot (SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a'_{0,0}))$$

$$= x \cdot (SBox(2 \circ x_{0,0}) \circ SBox(2 \circ x'_{0,0}))$$

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,1} = x \cdot (SBox(2 \circ x + a_{1,0}) \circ SBox(2 \circ x' + a'_{1,0}))$$

$$= x \cdot (SBox(2 \circ x_{1,0}) \circ SBox(2 \circ x'_{1,0}))$$

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,2} = x \cdot (SBox(2 \circ x + a_{2,0}) \circ SBox(2 \circ x' + a'_{2,0}))$$

$$= x \cdot (SBox(2 \circ x_{2,0}) \circ SBox(2 \circ x'_{2,0}))$$

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,3} = x \cdot (SBox(2 \circ x + a_{3,0}) \circ SBox(2 \circ x' + a'_{3,0}))$$

$$= x \cdot (SBox(2 \circ x_{3,0}) \circ SBox(2 \circ x'_{3,0}))$$

The two definitions of  $y^2$  and  $y'^2$  are defined equivalently that  $(Ry^2 \circ Ry^2 \circ D_J)_{1,0}$ ,  $(Ry'^2 \circ Ry'^2 \circ D_J)_{1,0}$ . The same holds for the other columns. Note that the entries of the two-revision  $y^2$  and  $y'^2$  is influenced by the fact that we are working in the entire case of  $D_J$ . This implies that the number of collisions must be that in a multiple of 2.

Question: given  $y^2 \circ D_J$  for  $|J| \geq 2$ , how again becomes the branch number of the MixColumns operation. In fact, indeed, composition  $(SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1})$  and analyze the first column (the others are analogous).

$$(SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) = \begin{bmatrix} SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a') \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

After the MixColumns operation, since three input bytes  $0$  are different from zero, it follows that at least two output bytes must be different from zero, in other words that  $Ry^2 \circ Ry^2 \circ D_J \in D_J$  for  $|J| \geq 2$  and only if  $a = a'$ , that is  $y = y'$ .

Note that  $SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a')$  and  $SBox(2 \circ x + a_{1,0}) \circ SBox(2 \circ x' + a')$  are equal only if  $x = x'$  and  $a = a'$ , which can never happen by hypothesis.

For completeness, it is also possible to show the same result in a different way. By definition,  $Ry^2 \circ Ry^2 \circ D_J$  for a certain  $J$  with  $|J| \geq 2$  and  $a \in M_{2^k} \times C_{2^k}$  is  $\{0\}$  for each  $x, x', y, y', z, z', w, w'$ . In fact, the four bytes of the diagonal group  $D_J$  are equal to zero, when the indices are taken with  $a$  and  $J$  in  $\{0, 1, 2, 3\}$ . As we are going to show, that is not the only way of that this case and since the branch number of the MixColumns operation is 5, it follows that  $Ry^2 \circ Ry^2 \circ D_J$  for the  $J$  with  $|J| \geq 2$ . In other words  $Ry^2 \circ Ry^2 \circ D_J$  for  $|J| \geq 2$  and only if  $a = a'$ , that is  $y = y'$ .

This implies that the two-revision  $y^2$  (generated by  $(x, y^2)$ ) and  $y'^2$  (generated by  $(x', y'^2)$ )

$$y^2 = x \begin{bmatrix} x' & y' & 0 & 0 \\ x' & y' & 0 & 0 \\ x' & y' & 0 & 0 \\ x' & y' & 0 & 0 \end{bmatrix}, \quad y'^2 = x' \begin{bmatrix} x & y & 0 & 0 \\ x & y & 0 & 0 \\ x & y & 0 & 0 \\ x & y & 0 & 0 \end{bmatrix}$$

belong to the same set of  $D_J$  after one round. To prove this fact, it is sufficient to compute  $Ry^2 \circ Ry^2 \circ D_J$  and  $Ry'^2 \circ Ry'^2 \circ D_J$ , and to prove that they are equal.

$$Ry^2 \circ Ry^2 \circ D_J = Ry'^2 \circ Ry'^2 \circ D_J$$

Since  $Ry^2 \circ Ry^2 \circ D_J \in D_J$ , it also follows that  $Ry'^2 \circ Ry'^2 \circ D_J$  is partitioned by simple composition the first column of  $Ry^2 \circ Ry^2 \circ D_J$  is given by:

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,0} = x \cdot (SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a'_{0,0}))$$

$$= x \cdot (SBox(2 \circ x_{0,0}) \circ SBox(2 \circ x'_{0,0}))$$

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,1} = x \cdot (SBox(2 \circ x + a_{1,0}) \circ SBox(2 \circ x' + a'_{1,0}))$$

$$= x \cdot (SBox(2 \circ x_{1,0}) \circ SBox(2 \circ x'_{1,0}))$$

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,2} = x \cdot (SBox(2 \circ x + a_{2,0}) \circ SBox(2 \circ x' + a'_{2,0}))$$

$$= x \cdot (SBox(2 \circ x_{2,0}) \circ SBox(2 \circ x'_{2,0}))$$

$$(Ry^2 \circ Ry^2 \circ D_J)_{1,3} = x \cdot (SBox(2 \circ x + a_{3,0}) \circ SBox(2 \circ x' + a'_{3,0}))$$

$$= x \cdot (SBox(2 \circ x_{3,0}) \circ SBox(2 \circ x'_{3,0}))$$

The two definitions of  $y^2$  and  $y'^2$  are defined equivalently that  $(Ry^2 \circ Ry^2 \circ D_J)_{1,0}$ ,  $(Ry'^2 \circ Ry'^2 \circ D_J)_{1,0}$ . The same holds for the other columns. Note that the entries of the two-revision  $y^2$  and  $y'^2$  is influenced by the fact that we are working in the entire case of  $D_J$ . This implies that the number of collisions must be that in a multiple of 2.

Question: given  $y^2 \circ D_J$  for  $|J| \geq 2$ , how again becomes the branch number of the MixColumns operation. In fact, indeed, composition  $(SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1})$  and analyze the first column (the others are analogous).

In  $x = x'$  and  $(x, y^2, y'^2) = (x', y'^2, y'^2)$  for each possible value of  $x$  and  $y$ , the result  $Ry^2 \circ Ry^2 \circ D_J \in D_J$ . In other words, the outcome of these elements is generated by the fact that we are working with the entire case of  $M_{2^k}$ .

**Fourth case.** Similarly, we consider the case in which all the variables are different, that is, for example, we assume that  $x = x', y = y', w = w'$  and  $a = a'$  (the other cases are analogous). Thus, we suppose that the two  $y$  and  $y'$  belong to the same set of  $M_{2^k} \times C_{2^k}$ , where  $a \in (M_{2^k} \times C_{2^k})$ .

Since  $M_{2^k} \times C_{2^k}$  is closed, it follows that  $x^2 y^2 y'^2 \in C_{2^k}$ , then  $Ry^2 \circ Ry^2 \circ Ry^2 \circ Ry^2 \circ Ry^2 \in \{0\}$  for each  $J$  and  $J'$  with  $|J| \geq 2$  and  $|J'| \geq 2$ . In other words, the given hyperplane for this case, it is not possible that the two bytes belong to the same set of a diagonal group  $D_J$  for each  $J$ . It also can be proved.

For completeness, it is also possible to show the same result in a different way. By definition,  $Ry^2 \circ Ry^2 \circ D_J$  for a certain  $J$  with  $|J| \geq 2$  and  $a \in M_{2^k} \times C_{2^k}$  is  $\{0\}$  for each  $x, x', y, y', z, z', w, w'$ . In fact, the four bytes of the diagonal group  $D_J$  are equal to zero, when the indices are taken with  $a$  and  $J$  in  $\{0, 1, 2, 3\}$ . As we are going to show, that is not the only way of that this case and since the branch number of the MixColumns operation is 5, it follows that  $Ry^2 \circ Ry^2 \circ D_J$  for the  $J$  with  $|J| \geq 2$ . In other words  $Ry^2 \circ Ry^2 \circ D_J$  for  $|J| \geq 2$  and only if  $a = a'$ , that is  $y = y'$ .

This implies that the two-revision  $y^2$  (generated by  $(x, y^2)$ ) and  $y'^2$  (generated by  $(x', y'^2)$ )

$$(SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) = \begin{bmatrix} SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a') \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

After the MixColumns operation, since three input bytes  $0$  are different from zero, it follows that at least two output bytes must be different from zero, in other words that  $Ry^2 \circ Ry^2 \circ D_J \in D_J$  for  $|J| \geq 2$  and only if  $a = a'$ , that is  $y = y'$ .

Note that  $SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a')$  and  $SBox(2 \circ x + a_{1,0}) \circ SBox(2 \circ x' + a')$  are equal only if  $x = x'$  and  $a = a'$ , which can never happen by hypothesis.

For completeness, it is also possible to show the same result in a different way. By definition,  $Ry^2 \circ Ry^2 \circ D_J$  for a certain  $J$  with  $|J| \geq 2$  and  $a \in M_{2^k} \times C_{2^k}$  is  $\{0\}$  for each  $x, x', y, y', z, z', w, w'$ . In fact, the four bytes of the diagonal group  $D_J$  are equal to zero, when the indices are taken with  $a$  and  $J$  in  $\{0, 1, 2, 3\}$ . As we are going to show, that is not the only way of that this case and since the branch number of the MixColumns operation is 5, it follows that  $Ry^2 \circ Ry^2 \circ D_J$  for the  $J$  with  $|J| \geq 2$ . In other words  $Ry^2 \circ Ry^2 \circ D_J$  for  $|J| \geq 2$  and only if  $a = a'$ , that is  $y = y'$ .

This implies that the two-revision  $y^2$  (generated by  $(x, y^2)$ ) and  $y'^2$  (generated by  $(x', y'^2)$ )

$$(SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) \circ (SBox \circ SBox^{-1}) = \begin{bmatrix} SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a') \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

After the MixColumns operation, since three input bytes  $0$  are different from zero, it follows that at least two output bytes must be different from zero, in other words that  $Ry^2 \circ Ry^2 \circ D_J \in D_J$  for  $|J| \geq 2$  and only if  $a = a'$ , that is  $y = y'$ .

Note that  $SBox(2 \circ x + a_{0,0}) \circ SBox(2 \circ x' + a')$  and  $SBox(2 \circ x + a_{1,0}) \circ SBox(2 \circ x' + a')$  are equal only if  $x = x'$  and  $a = a'$ , which can never happen by hypothesis.



## Our contribution starts here

- ▶ Search for the underlying property ;
- ▶ write a better proof for it to come out;
- ▶ generalize ?

## Step 1: equivalence relation between pairs

In  $\mathcal{M}_0$ ,

$$\left\{ \left( \begin{pmatrix} 2 \cdot x_0 & x_1 & z_2 & 3 \cdot z_3 \\ x_0 & x_1 & 3 \cdot z_2 & 2 \cdot z_3 \\ x_0 & 3 \cdot x_1 & 2 \cdot z_2 & z_3 \\ 3 \cdot x_0 & 2 \cdot x_1 & z_2 & z_3 \end{pmatrix}, \begin{pmatrix} 2 \cdot y_0 & y_1 & z_2 & 3 \cdot z_3 \\ y_0 & y_1 & 3 \cdot z_2 & 2 \cdot z_3 \\ y_0 & 3 \cdot y_1 & 2 \cdot z_2 & z_3 \\ 3 \cdot y_0 & 2 \cdot y_1 & z_2 & z_3 \end{pmatrix} \right) \right\}$$

$$\sim$$

$$\left\{ \left( \begin{pmatrix} 2 \cdot x_0 & y_1 & w_2 & 3 \cdot w_3 \\ x_0 & y_1 & 3 \cdot w_2 & 2 \cdot w_3 \\ x_0 & 3 \cdot y_1 & 2 \cdot w_2 & w_3 \\ 3 \cdot x_0 & 2 \cdot y_1 & w_2 & w_3 \end{pmatrix}, \begin{pmatrix} 2 \cdot y_0 & x_1 & w_2 & 3 \cdot w_3 \\ y_0 & x_1 & 3 \cdot w_2 & 2 \cdot w_3 \\ y_0 & 3 \cdot x_1 & 2 \cdot w_2 & w_3 \\ 3 \cdot y_0 & 2 \cdot x_1 & w_2 & w_3 \end{pmatrix} \right) \right\}$$

$$\left\{ \left( \begin{array}{cccc} 2 \cdot x_0 & x_1 & z_2 & 3 \cdot z_3 \\ x_0 & x_1 & 3 \cdot z_2 & 2 \cdot z_3 \\ x_0 & 3 \cdot x_1 & 2 \cdot z_2 & z_3 \\ 3 \cdot x_0 & 2 \cdot x_1 & z_2 & z_3 \end{array} \right), \left( \begin{array}{cccc} 2 \cdot y_0 & y_1 & z_2 & 3 \cdot z_3 \\ y_0 & y_1 & 3 \cdot z_2 & 2 \cdot z_3 \\ y_0 & 3 \cdot y_1 & 2 \cdot z_2 & z_3 \\ 3 \cdot y_0 & 2 \cdot y_1 & z_2 & z_3 \end{array} \right) \right\}$$

 $\sim$ 

$$\left\{ \left( \begin{array}{cccc} 2 \cdot x_0 & y_1 & w_2 & 3 \cdot w_3 \\ x_0 & y_1 & 3 \cdot w_2 & 2 \cdot w_3 \\ x_0 & 3 \cdot y_1 & 2 \cdot w_2 & w_3 \\ 3 \cdot x_0 & 2 \cdot y_1 & w_2 & w_3 \end{array} \right), \left( \begin{array}{cccc} 2 \cdot y_0 & x_1 & w_2 & 3 \cdot w_3 \\ y_0 & x_1 & 3 \cdot w_2 & 2 \cdot w_3 \\ y_0 & 3 \cdot x_1 & 2 \cdot w_2 & w_3 \\ 3 \cdot y_0 & 2 \cdot x_1 & w_2 & w_3 \end{array} \right) \right\}$$

### Definition

Let  $\{p^0, p^1\}$  a pair of states from  $\mathcal{M}_I + a$ . The **information set**  $K$  of the pair  $\{p^0, p^1\}$  is  $\{k \in \llbracket 0, 3 \rrbracket \mid \exists i \in I : x_{i,k} \neq y_{i,k}\}$ .

It is  $K = \{0, 1\}$  in the example.

$$\left\{ \left( \begin{array}{cccc} 2 \cdot x_0 & x_1 & z_2 & 3 \cdot z_3 \\ x_0 & x_1 & 3 \cdot z_2 & 2 \cdot z_3 \\ x_0 & 3 \cdot x_1 & 2 \cdot z_2 & z_3 \\ 3 \cdot x_0 & 2 \cdot x_1 & z_2 & z_3 \end{array} \right), \left( \begin{array}{cccc} 2 \cdot y_0 & y_1 & z_2 & 3 \cdot z_3 \\ y_0 & y_1 & 3 \cdot z_2 & 2 \cdot z_3 \\ y_0 & 3 \cdot y_1 & 2 \cdot z_2 & z_3 \\ 3 \cdot y_0 & 2 \cdot y_1 & z_2 & z_3 \end{array} \right) \right\}$$

$$\sim$$

$$\left\{ \left( \begin{array}{cccc} 2 \cdot x_0 & y_1 & w_2 & 3 \cdot w_3 \\ x_0 & y_1 & 3 \cdot w_2 & 2 \cdot w_3 \\ x_0 & 3 \cdot y_1 & 2 \cdot w_2 & w_3 \\ 3 \cdot x_0 & 2 \cdot y_1 & w_2 & w_3 \end{array} \right), \left( \begin{array}{cccc} 2 \cdot y_0 & x_1 & w_2 & 3 \cdot w_3 \\ y_0 & x_1 & 3 \cdot w_2 & 2 \cdot w_3 \\ y_0 & 3 \cdot x_1 & 2 \cdot w_2 & w_3 \\ 3 \cdot y_0 & 2 \cdot x_1 & w_2 & w_3 \end{array} \right) \right\}$$

### Definition

Let  $P = \{p^0, p^1\}$ ,  $Q = \{q^0, q^1\} \in \mathcal{P}^2(\mathcal{M}_I + a)$ . We have  $P \sim Q$  if:

- ▶  $K$  is the information set of  $P \Rightarrow K$  is the information set of  $Q$ .
- ▶  $\forall k \in K, \exists b \in \{0, 1\} : \forall i \in I, q_{i,k}^0 = p_{i,k}^b$  et  $q_{i,k}^1 = p_{i,k}^{1-b}$ .

$\sim$  is an equivalence relation on  $\mathcal{P}^2(\mathcal{M}_I + a)$ .

## Lemma

The function

$$f : \mathcal{P}^2(\mathcal{M}_l + a) \longrightarrow \mathcal{M}_4(\mathbb{K})$$

$$\{p^0, p^1\} \longmapsto \mathcal{R}(p^0) + \mathcal{R}(p^1)$$

is constant on the equivalence classes of  $\sim$ .

## Proposition

Let  $\mathcal{C}$  be an equivalence class  $K$ . Then

$$\#\mathcal{C} = 2^{|K|-1+8|l|(4-|K|)} \equiv 0 \pmod{8}.$$

## Lemma

If

$$n = \#\{ \{p^0, p^1\} \in \mathcal{P}^2(\mathcal{M}_I + a) \mid \mathcal{R}(p^0) + \mathcal{R}(p^1) \in \mathcal{D}_J \},$$

then  $n \equiv 0 \pmod{8}$ .

Proof.

$$\begin{aligned} n &= \#f^{-1}(\mathcal{D}_J) \\ &= \sum_{\mathfrak{c} \in \mathcal{P}^2(\mathcal{M}_I + a) / \sim} \#(f^{-1}(\mathcal{D}_J) \cap \mathfrak{c}) \\ &= \sum_{\mathfrak{c} \in \mathcal{P}^2(\mathcal{M}_I + a) / \sim} 1_{\tilde{f}(\mathfrak{c}) \in \mathcal{D}_J} \#\mathfrak{c} \\ &\equiv 0 \pmod{8} \end{aligned}$$



## What about the branch number ?

In [GRR17], the proof needs maximal branch number. But...

### Proposition ([GRR16])

Let  $I, J \subseteq \llbracket 0, 3 \rrbracket$  and  $b$  be the differential branch number of MC. Then

$$|I| + |J| < b \quad \Rightarrow \quad \mathcal{D}_I \cap \mathcal{M}_J = \{0\}$$

If  $\{p^0, p^1\} \in \mathcal{P}^2(\mathcal{M}_I + a)$  has information set  $K$ ,

$$p^0 + p^1 \in \mathcal{C}_K \text{ and then } \mathcal{R}(p^0) + \mathcal{R}(p^1) \in \mathcal{M}_K.$$

If  $|K| < b - |J|$ ,  $\mathcal{M}_K \cap \mathcal{D}_J = \{0\}$  and  $\mathcal{R}(p^0) + \mathcal{R}(p^1) \notin \mathcal{D}_J$ .

## Lemma

If

$$n = \#\{ \{p^0, p^1\} \in \mathcal{P}^2(\mathcal{M}_I + a) \mid \mathcal{R}(p^0) + \mathcal{R}(p^1) \in \mathcal{D}_J \},$$

then  $n \equiv 0 \pmod{8}$ .

Proof.

$$\begin{aligned} n &= \sum_{\mathfrak{c} \in \mathcal{P}^2(\mathcal{M}_I + a) / \sim} 1_{\tilde{f}(\mathfrak{c}) \in \mathcal{D}_J} \#\mathfrak{c} \\ &= \sum_{h=0}^4 \sum_{\mathfrak{c}: |K(\mathfrak{c})|=h} 1_{\tilde{f}(\mathfrak{c}) \in \mathcal{D}_J} \#\mathfrak{c} \\ &= \sum_{h=b-|J|}^4 \sum_{\mathfrak{c}: |K(\mathfrak{c})|=h} 1_{\tilde{f}(\mathfrak{c}) \in \mathcal{D}_J} \#\mathfrak{c} \end{aligned}$$



The AES and the distinguisher of [GRR17]

Proof for the distinguisher

Case of the AES

Towards a more general lemma

Example on another SPN: Midori

Conclusion



$$\begin{pmatrix} 2 \\ 1 \\ 1 \\ 3 \\ \\ 1 \\ 1 \\ 3 \\ 2 \\ \\ 1 \\ 3 \\ 2 \\ 1 \\ \\ 3 \\ 2 \\ 1 \\ 1 \end{pmatrix}$$

$\mathcal{M}_0$  is compatible with  $\mathcal{S}_{AES}$ .

Likewise,  $\mathcal{M}_0 \cap \mathcal{C}_{0,1}$  is compatible with  $\mathcal{S}_{AES}$ .

$$\begin{pmatrix} 2 \cdot x_0 & x_1 & 0 & 0 \\ x_0 & x_1 & 0 & 0 \\ x_0 & 3 \cdot x_1 & 0 & 0 \\ 3 \cdot x_0 & 2 \cdot x_1 & 0 & 0 \end{pmatrix} \in \mathcal{M}_0 \cap \mathcal{C}_{0,1}.$$

The AES and the distinguisher of [GRR17]

Proof for the distinguisher

Case of the AES

Towards a more general lemma

Example on another SPN: Midori

Conclusion

# Midori

Midori, presented at Asiacrypt 2015 [BBI<sup>+</sup>15].

Goal: low energy consumption.

- ▶  $\mathcal{R} : \mathbb{F}_2^{128} \rightarrow \mathbb{F}_2^{128}$
- ▶ S-box:  $\mathbb{F}_{2^8} \rightarrow \mathbb{F}_{2^8}$
- ▶  $\mathcal{L}$  :
  - ▶ ShuffleCell  $SC$  (more complex ShiftRows)
  - ▶ MixColumns  $MC$

$$M_{MC} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$\underbrace{\mathcal{D}'_I \xRightarrow{\mathcal{R}} C_I \xRightarrow{\mathcal{R}} \mathcal{M}'_I}_{2} \xrightarrow[\mathcal{R}]{\text{Generalized Lemma } 1} \mathcal{D}'_J \xRightarrow{\mathcal{R}} C_J \xRightarrow{\mathcal{R}} \mathcal{M}'_J$$

## The AES and the distinguisher of [GRR17]

The AES

The distinguisher of Grassi, Rechberger and Rønjom

## Proof for the distinguisher

Case of the AES

Towards a more general lemma

Example on another SPN: Midori

## Conclusion

## What now ?

- ▶ The generalization can be useful (the distinguisher can be easily transposed)  
but cannot give better results!
- ▶ Working on subspace trails [LTW18].

$$\underbrace{D'_I \xrightarrow{\mathcal{R}} C_I \xrightarrow{\mathcal{R}} M'_I}_2 \xrightarrow[\mathcal{R}]{\text{Generalized Lemma}} \underbrace{D'_J \xrightarrow{\mathcal{R}} C_J \xrightarrow{\mathcal{R}} M'_J}_2$$



S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, and T. Akishita.

Midori: A block cipher for low energy.

In *ASIACRYPT 2015 (2)*, pages 411 – 436, 2015.



J. Daemen and V. Rijmen.

*The Design of Rijndael: AES - The Advanced Encryption Standard*.  
Springer, 2002.



L. Grassi, C. Rechberger, and S. Rønjom.

Subspace trail cryptanalysis and its applications to AES.

*IACR Trans. Symmetric Cryptol.*, 2016(2):192–225, 2016.



L. Grassi, C. Rechberger, and S. Rønjom.

A new structural-differential property of 5-round AES.

In *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 289–317. Springer, 2017.



G. Leander, C. Tezcan, and F. Wiemer.

Searching for subspace trails and truncated differentials.



*IACR Trans. Symmetric Cryptol.*, 2018(1):74–100, 2018.