

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://inria.hal.science/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 Rønjor

Proof for the distinguisher

Conclusion

The AES

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

$$x = \begin{pmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{pmatrix} \in \mathbb{F}_{2^8}^{16} \qquad \text{S-box } \begin{cases} \mathbb{F}_{2^8} \to \mathbb{F}_{2^8} \\ x_i & \mapsto & y_i \end{cases}$$

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

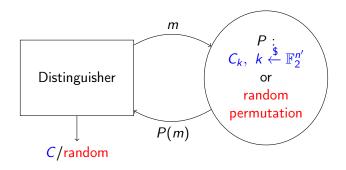
$$MC(z) = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \times z \qquad \text{MixColumns } MC$$

The AES and the distinguisher of [GRR17]

The distinguisher of Grassi, Rechberger and Rønjom

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...

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

$$\begin{pmatrix} x_0 & 0 & 0 & 0 \\ x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{C}_0 \qquad \qquad \begin{array}{c} \text{Columns} \\ \mathcal{C}_i = \text{vect}_{\mathbb{K}}(e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i}) \\ \end{array}$$

$$\begin{pmatrix} 0 & x_0 & 0 & y_0 \\ 0 & x_1 & 0 & y_1 \\ 0 & x_2 & 0 & y_2 \\ 0 & x_3 & 0 & y_3 \end{pmatrix} \in \mathcal{C}_{\{1,3\}} \qquad I \subseteq \llbracket 0, 3 \rrbracket : \\ \mathcal{C}_I = \bigoplus_{i \in I} \mathcal{C}_i.$$

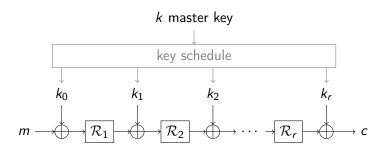
$$\begin{pmatrix} x_0 & 0 & 0 & 0 \\ 0 & x_1 & 0 & 0 \\ 0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & x_3 \end{pmatrix} \in \mathcal{D}_0, \qquad \begin{array}{l} \text{Diagonals:} \\ \mathcal{D}_i = SR^{-1}(\mathcal{C}_i) \\ \end{pmatrix}$$

$$\begin{pmatrix} x_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_1 \\ 0 & 0 & x_2 & 0 \\ 0 & x_3 & 0 & 0 \end{pmatrix} \in \mathcal{ID}_0, \qquad \begin{array}{l} \text{Anti-diagonals:} \\ \mathcal{ID}_i = SR(\mathcal{C}_i) \\ \end{pmatrix}$$

$$\begin{pmatrix} 2 \cdot x_0 & x_1 & x_2 & 3 \cdot x_3 \\ x_0 & x_1 & 3 \cdot x_2 & 2 \cdot x_3 \\ x_0 & 3 \cdot x_1 & 2 \cdot x_2 & x_3 \\ 3 \cdot x_0 & 2 \cdot x_1 & x_2 & x_3 \\ \end{pmatrix} \in \mathcal{M}_0. \qquad \begin{array}{l} \text{Mixed:} \\ \mathcal{M}_i = MC(\mathcal{ID}_i) \\ \end{pmatrix}$$

$$\mathcal{D}_{I} \xrightarrow{\mathcal{S}} \mathcal{D}_{I} \xrightarrow{SR} \mathcal{C}_{I} \xrightarrow{MC} \mathcal{C}_{I} \xrightarrow{\mathcal{S}} \mathcal{C}_{I} \xrightarrow{SR} \mathcal{I}\mathcal{D}_{I} \xrightarrow{MC} \mathcal{M}_{I}$$

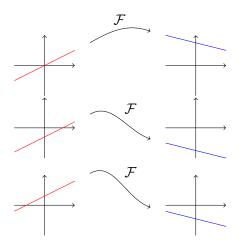
The AES is a key-alternating blockcipher



Subspace trails

Definition ([LTW18])

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



Examples:

- $\blacktriangleright \{0\} \stackrel{\mathcal{F}}{\rightrightarrows} \{0\}$
- $V \stackrel{\mathcal{F}}{\Rightarrow} \mathbb{K}^N$

$$\mathcal{D}_0 \stackrel{\mathcal{R}}{\rightrightarrows} \mathcal{C}_0$$
 $\forall a, \forall x,$

$$\begin{pmatrix}
x_0 & 0 & 0 & 0 \\
0 & x_1 & 0 & 0 \\
0 & 0 & x_2 & 0 \\
0 & 0 & 0 & x_3
\end{pmatrix}
\xrightarrow{+a}
\begin{pmatrix}
x_0 + a_0 & * & * & * \\
* & x_1 + a_1 & * & * \\
* & * & x_2 + a_2 & * \\
* & * & * & * & * \\
* & * & * & * & * & *
\end{pmatrix}$$

$$\xrightarrow{S}
\begin{pmatrix}
y_0 & * & * & * \\
* & y_1 & * & * \\
* & * & y_2 & * \\
* & * & * & * & *
\end{pmatrix}
\xrightarrow{SR}
\begin{pmatrix}
y_0 & * & * & * \\
y_1 & * & * & * \\
y_2 & * & * & * \\
y_3 & * & * & *
\end{pmatrix}$$

$$\xrightarrow{MC}
\begin{pmatrix}
\vdots & * & * & * \\
\vdots & * & * & * \\
MC(y) & * & * & * \\
\vdots & * & * & * \\
\vdots & * & * & *
\end{pmatrix}$$

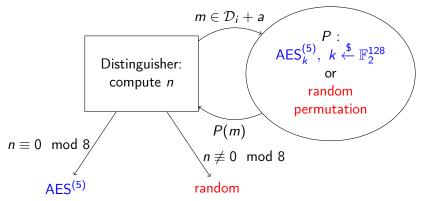
The distinguisher

Theorem ([GRR17])

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

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

Then $n \equiv 0 \mod 8$.



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 $a \in \mathcal{M}_4(\mathbb{K}), I \subset [0,3], J \subseteq [0,3]$. We define

$$n=\#\{\ \{p^0,p^1\}\in\mathcal{P}^2(\textcolor{red}{\mathcal{M}_{\textit{I}}}+a)\mid \mathcal{R}(p^0)+\mathcal{R}(p^1)\in\textcolor{red}{\mathcal{D}_{\textit{J}}}\}.$$

Then $n \equiv 0 \mod 8$.

Proof

In the original paper [GRR17]:

First case. First, we consider the case in which three variables are ear

$$(SRe \; S \; \text{Hom}[p^2] \otimes SRe \; S \; \text{Hom}[p^2])_{i,0} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$
 After the MixColumns operation (note $R[p^2] \otimes R[p^2] = MC(SRe \; S \; B$

 $[S \operatorname{Box}(2 \cdot x \oplus a_{0,k}) \oplus S \operatorname{Box}(2 \cdot x' \oplus .$

After the MixColumns operation (note $R(s^1) \cap R(s^2) = MC(SR + S Rox(s^1))$ must be different from zero, that is all the output bytes are different from ze

that is w.l.o.g. we assume for example that z = z' and w = w', while $x \neq z'$

The state of the Same $(2 \cdot \sigma \oplus \omega_{0,0}) \oplus S$ dive $(2 \cdot \sigma' \oplus \omega_{0,0}) = 0$ if and only if $\sigma = \sigma'$, wi

$$\vec{p}^2 = a \odot \begin{bmatrix} 2 \cdot x' & y & 0 & 0 \\ x' & y & 0 & 0 \\ x' & 2 \cdot y & 0 & 0 \\ 1 \cdot x' & 2 \cdot y & 0 & 0 \end{bmatrix} , \qquad \vec{p}^2 = a \odot \begin{bmatrix} 2 \cdot x & y' & 0 & 0 \\ x & y' & 0 & 0 \\ x & 2 \cdot y' & 0 & 0 \\ 3 \cdot x & 2 \cdot y' & 0 & 0 \end{bmatrix}$$

 $B(s^2) = B(s^2) = B(s^2) = B(s^2).$

 $(R(p^2) \oplus R(p^2))_{AB} = 2 \cdot (S \operatorname{disc}(2 \cdot x \oplus a_{AB}) \oplus S \operatorname{disc}(2 \cdot x' \oplus a_{AB})) \oplus$ $\odot 3 \cdot (S \cdot \operatorname{Box}[g \odot a_{1,1}) \odot S \cdot \operatorname{Box}[g' \odot a_{2,1})).$ $(R(p^2) \oplus R(p^2))_{1:0} = S \operatorname{Box}(2 \cdot x \oplus a_{0:0}) \oplus S \operatorname{Box}(2 \cdot x' \oplus a_{0:0}) \oplus$

 $\oplus 2 \cdot (S \cdot \operatorname{Box}(y \oplus a_{1,1}) \oplus S \cdot \operatorname{Box}(y' \oplus a_{2,1})).$ $(R(p^1) \oplus R(p^2)) \circ a = \operatorname{S-Box}(2 \cdot a \oplus \operatorname{on} a) \oplus \operatorname{S-Box}(2 \cdot a' \oplus \operatorname{on} a) \oplus$ $\odot S \operatorname{Bas}(y \odot a_{1,1}) \odot S \operatorname{Bas}(y' \odot a_{1,1}).$ $(R(p^1) \oplus R(p^2))_{1,0} = 2 \cdot (S \operatorname{disc}(2 \cdot x \oplus a_{0,0}) \oplus S \operatorname{disc}(2 \cdot x' \oplus a_{0,0})) \oplus$ m S-Block mas a) m S-Books' mas a).

Due to the definition of \hat{p}^1 and \hat{p}^2 , it follows immediately that $(R(p^1) \cap R(p^2))$ time: given p^a and p^b as before, is it possible that x, y, x', y' exist n

$$(SR:\operatorname{S-Ron}(p^2) \oplus SR:\operatorname{S-Ron}(p^2))_{,,0} = \begin{bmatrix} \operatorname{S-Ron}(2 \cdot x \odot a_{0,0}) \oplus \operatorname{S-Ron}(2 \cdot x' \odot x \odot x \odot x) \\ \operatorname{S-Ron}(p \odot a_{1,0}) \oplus \operatorname{S-Ron}(p' \odot a_{1,0}) \\ 0 \\ 0 \end{bmatrix}$$

After the MistColumns operation (note $R(s^1) \cap R(s^2) = MC(SR + S \operatorname{Box}(s^2))$ $SR \circ S \operatorname{-Hom}(p^2)()$, since two input bytes 11 are different from zero, it follows t Note that 8 libes $(2 \cdot \sigma \oplus m_1 s) \oplus 8$ libes $(2 \cdot \sigma' \oplus m_1 s) = 0$ if and only if $\sigma = \sigma'$, which never happen for hypothesis. In the same map, 8 libes $(g \oplus n_{r,j}) \oplus 8$ libes $(g' \oplus n_{r,j})$

This implies that the two elements if (emerated by (a, w/i) and if (evens) — at least three context bytes must be different from zero, or at most one output

with the previous conditions. Moreover, observe that $R(p^1) \oplus R(p^2) \oplus D_J$ for |J| = 3 if and only if is better (one nor column) of $R(p^1) \oplus R(p^2)$ are equal to zero. Since there are is "free" variables (i.e. x, y, x', y') and a system of four equations, such a syst of 2^{nk} . Indeed, assume that for certain x one w over some x, y, y, y.

or

the true obscure y of x of y' of x of y' of

 $(R(p^k) \oplus R(p^k))_{i,i} = A_k \cdot (\operatorname{S-Box}(R_b \cdot x \oplus C_b) \oplus \operatorname{S-Box}(R_b \cdot x' \oplus C_b)) \oplus$ $\odot Az \cdot (S \cdot \operatorname{Bas}(Bz \cdot z \odot Cz) \odot S \cdot \operatorname{Bas}(Bz \cdot z' \odot Cz)) \odot$

 $\cap A_i \cdot (S \text{-Biss}(B_i \cdot w \cap C_i) \cap S \text{-Biss}(B_i \cdot w' \cap C_i)) =$ $=A_{n} \cdot (S \cdot Box(B_{n} \cdot x \cap C_{n}) \cap S \cdot Box(B_{n} \cdot x' \cap C_{n})) \cap$ $mA_i \cdot (S \operatorname{Bas}(B_i - v \cap C_i) \cap S \operatorname{Bas}(B_i - v' \cap C_i))$. It follows that - under the merrious brusthesis - such pair of elements of and

Third case. Third's, we consider the case in which only one variable is con-

After the MisColumns operation, since three input bytes¹² are different fo

this case, the idea is to show that the difference $R(u^*) = R(u^*)$ doesn't denom

 $(R(s^2) \cap R(s^2))$, $c = A_s \cdot (S \cdot Rox(B_s \cdot s \cap C_s) \cap S \cdot Rox(B_s \cdot s' \cap C_s))$ m As - (S-Box(B) - a m C) = S-Box(B) - a' m C) (m

It follows that - under the previous hypothesis - each pair of elements p^{λ} and Note that $S \operatorname{Bos}(2 \circ (m,s) \otimes S \operatorname{Bos}(2 \circ (m,s) = S \operatorname{Bos}(y \otimes m,s) \otimes S \operatorname{Bos}(y' \otimes m,s)$ (a. a. a. a) and (at at at a) for each possible value of a satisfy the conditi

Fourth case. Fourthly, we consider the case in which all the variables

for a total of eight different pairs. As before, in order to prove this fact it sufficient to show that $E(a^1) \cap E(a^2) \cap E(a^2) \cap E(a^2)$. Moreover, as before in with all the coset of Ato. This implies that the number of collisions must be

 $[S\text{-}Bou(2\cdot x\otimes a_{0:0})\otimes S\text{-}Bou(2\cdot x'\otimes x$ $(SB_1 \otimes Box(p^2) \otimes SB_2 \otimes Box(p^2))_{i,i} = \begin{cases} SBox(p^2 \otimes a_{i,k}) \otimes SBox(p^2 \otimes a_{i,k}) \\ SBox(p^2 \otimes a_{i,k}) \otimes SBox(p^2 \otimes a_{i,k}) \\ SBox(p^2 \otimes a_{i,k}) \otimes SBox(p^2 \otimes a_{i,k}) \end{cases}$

S-Busin mean) in S-Bostor' men

Note that \hat{S} $\operatorname{Bin}(2 \circ (\omega_{n,n}) \otimes \hat{S} \operatorname{Bin}(2 \circ (\omega_{n,n}) = S \operatorname{Bin}(g \otimes \omega_{n,n}) \otimes S \operatorname{Bin}(g' \otimes \omega_{n,n}) \otimes \operatorname{Bin}(g' \otimes \omega_{n,n}) \otimes \operatorname{Bin}(g' \otimes \omega_{n,n}) \otimes \operatorname{Bin}(g' \otimes \omega_{n,n}) = 0$ if

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 ,

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

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

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

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

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 $\{k \in [0, 3] \mid \exists i \in I : x_{i,k} \neq y_{i,k}\}$.

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

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

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

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.
- ▶ $\forall k \in K, \exists b \in \{0,1\} : \forall i \in I, q_{i,k}^0 = p_{i,k}^b \text{ et } q_{i,k}^1 = p_{i,k}^{1-b}.$
- \sim is an equivalence relation on $\mathcal{P}^2(\mathcal{M}_I + a)$.

Lemma

The function

$$\begin{array}{cccc} f: & \mathcal{P}^2(\mathcal{M}_I + a) & \longrightarrow & \mathcal{M}_4(\mathbb{K}) \\ & & \{p^0, p^1\} & \longmapsto & \mathcal{R}(p^0) + \mathcal{R}(p^1) \end{array}$$

is constant on the equivalence classes of \sim .

Proposition

Let C be an equivalence class K. Then

$$\#\mathfrak{C} = 2^{|K|-1+8|I|(4-|K|)} \equiv 0 \mod 8.$$

Lemma

lf

$$n=\#\{\;\{p^0,p^1\}\in\mathcal{P}^2(\mathcal{M}_I+a)\;|\;\mathcal{R}(p^0)+\mathcal{R}(p^1)\in\mathcal{D}_J\},$$
 then $n\equiv 0\mod 8$.

Proof.

$$n = \#f^{-1}(\mathcal{D}_J)$$

$$= \sum_{\mathfrak{C} \in \mathcal{P}^2(\mathcal{M}_I + a) / \sim} \#(f^{-1}(\mathcal{D}_J) \cap \mathfrak{C})$$

$$= \sum_{\mathfrak{C} \in \mathcal{P}^2(\mathcal{M}_I + a) / \sim} 1_{\tilde{f}(\mathfrak{C}) \in \mathcal{D}_J} \#\mathfrak{C}$$

$$\equiv 0 \mod 8$$

What about the branch number?

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

Proposition ([GRR16])

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

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

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

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

If
$$|K| < \frac{b}{b} - |J|$$
, $\mathcal{M}_K \cap \mathcal{D}_J = \{0\}$ and $\mathcal{R}(p^0) + \mathcal{R}(p^1) \not\in \mathcal{D}_J$.

Lemma

lf

$$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 $n \equiv 0 \mod 8$.

Proof.

$$n = \sum_{\mathfrak{C} \in \mathcal{P}^{2}(\mathcal{M}_{I} + a) / \sim} 1_{\tilde{f}(\mathfrak{C}) \in \mathcal{D}_{J}} \#\mathfrak{C}$$

$$= \sum_{h=0}^{4} \sum_{\mathfrak{C}: |K(\mathfrak{C})| = h} 1_{\tilde{f}(\mathfrak{C}) \in \mathcal{D}_{J}} \#\mathfrak{C}$$

$$= \sum_{h=b-|J|} \sum_{\mathfrak{C}: |K(\mathfrak{C})| = h} 1_{\tilde{f}(\mathfrak{C}) \in \mathcal{D}_{J}} \#\mathfrak{C}$$

Proof for the distinguisher

Towards a more general lemma

Example on another SPN: Midori

Definition

Let $V \subseteq \mathbb{K}^N$ be a \mathbb{K} -subspace. We say V is compatible with S if it has a basis g such that its matrix in basis f is of the form:

 \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+15]. Goal: low energy consumption.

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

$$M_{MC} = \left(\begin{array}{cccc} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{array}\right)$$



Conclusion

The AES and the distinguisher of [GRR17]

The AES

The distinguisher of Grassi, Rechberger and Rønjon

Proof for the distinguisher

Case of the AES

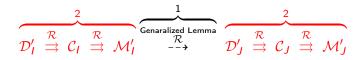
Towards a more general lemma

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].



- 🔋 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.

Conclusion

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