On subspace trails cryptanalysis

Daniel Coggia

On subspace trails cryptanalysis

Daniel Coggia

Inria Paris, Project Team SECRET

October 8, 2018

Outline

The AES

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

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

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

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

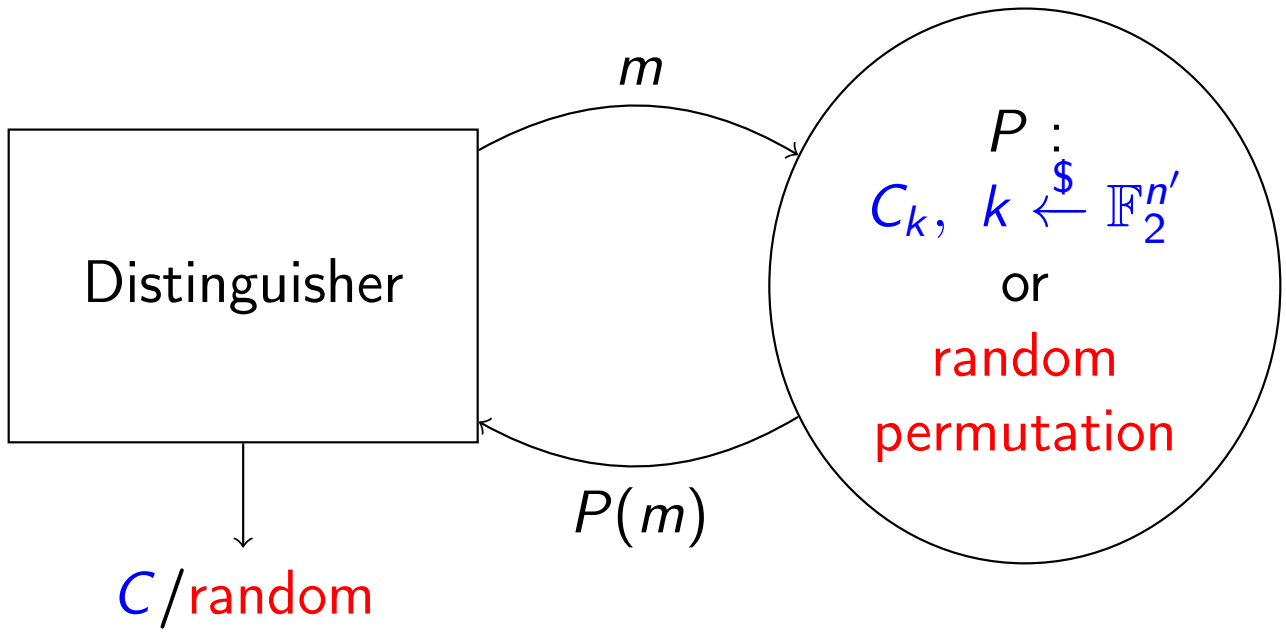
ShiftRows SR

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

MixColumns MC

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...

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

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

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

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

$I \subseteq [\![0, 3]\!]$:
$\mathcal{C}_I = \bigoplus_{i \in I} \mathcal{C}_i$.

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

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

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

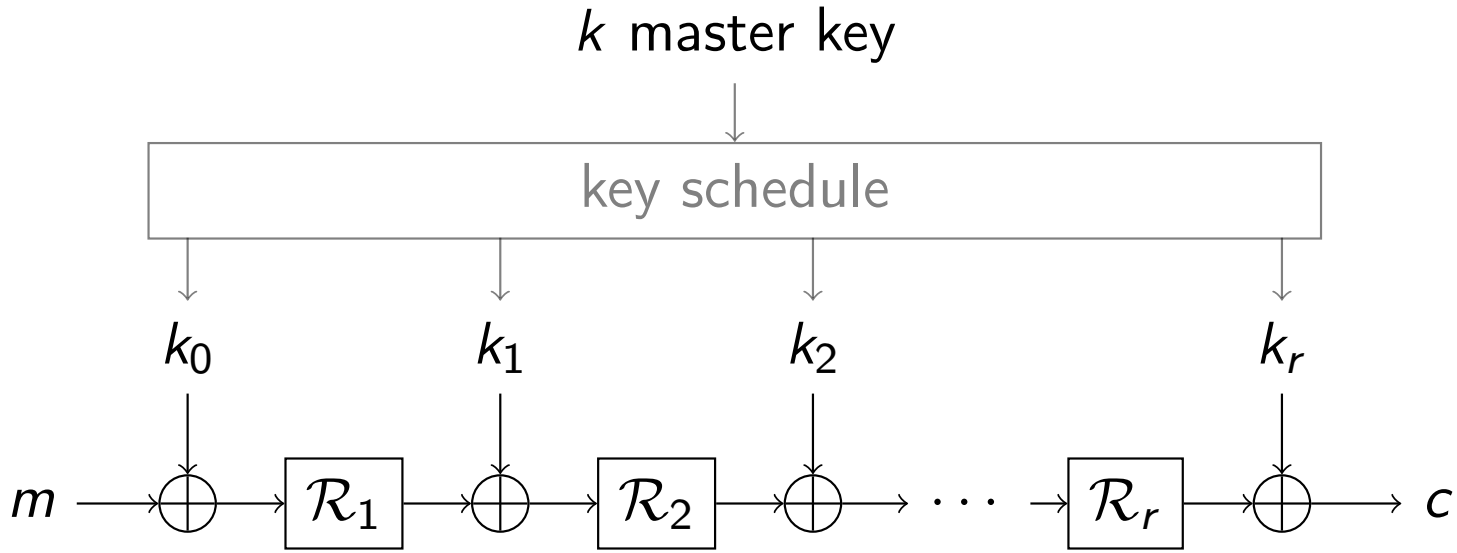
Anti-diagonals:
$\mathcal{ID}_i = SR(\mathcal{C}_i)$

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

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

$$\mathcal{D}_I \overbrace{\xrightarrow{\mathcal{S}} \mathcal{D}_I \xrightarrow{SR} \mathcal{C}_I \xrightarrow{MC}}^{\mathcal{R}} \mathcal{C}_I \overbrace{\xrightarrow{\mathcal{S}} \mathcal{C}_I \xrightarrow{SR} \mathcal{ID}_I \xrightarrow{MC}}^{\mathcal{R}} \mathcal{M}_I$$

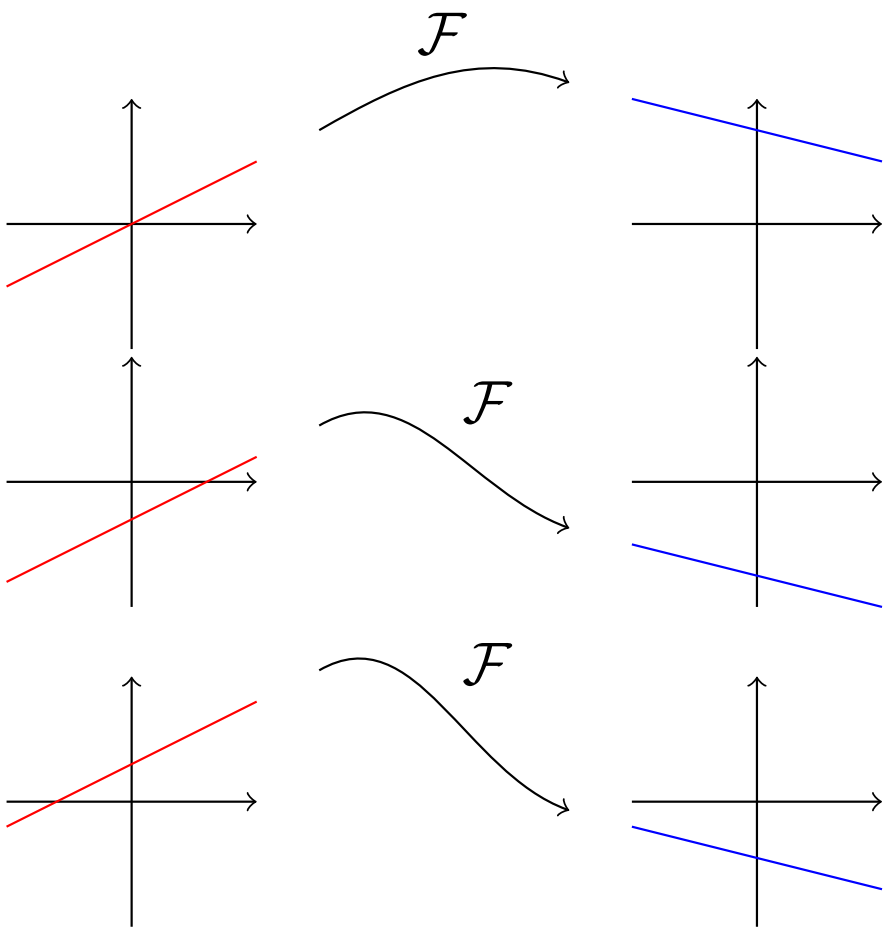
The AES is a key-alternating blockcipher



Subspace trails

Definition ([LTW18])

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



Examples:

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

$$\mathcal{D}_0 \overset{\mathcal{R}}{\rightrightarrows} \mathcal{C}_0$$

$\forall a, \forall x,$

$$\begin{pmatrix} x_0 & 0 & 0 & 0 \\ 0 & x_1 & 0 & 0 \\ 0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & x_3 \end{pmatrix} \xrightarrow{+a} \begin{pmatrix} x_0 + a_0 & * & * & * \\ * & x_1 + a_1 & * & * \\ * & * & x_2 + a_2 & * \\ * & * & * & x_3 + a_3 \end{pmatrix}$$

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

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

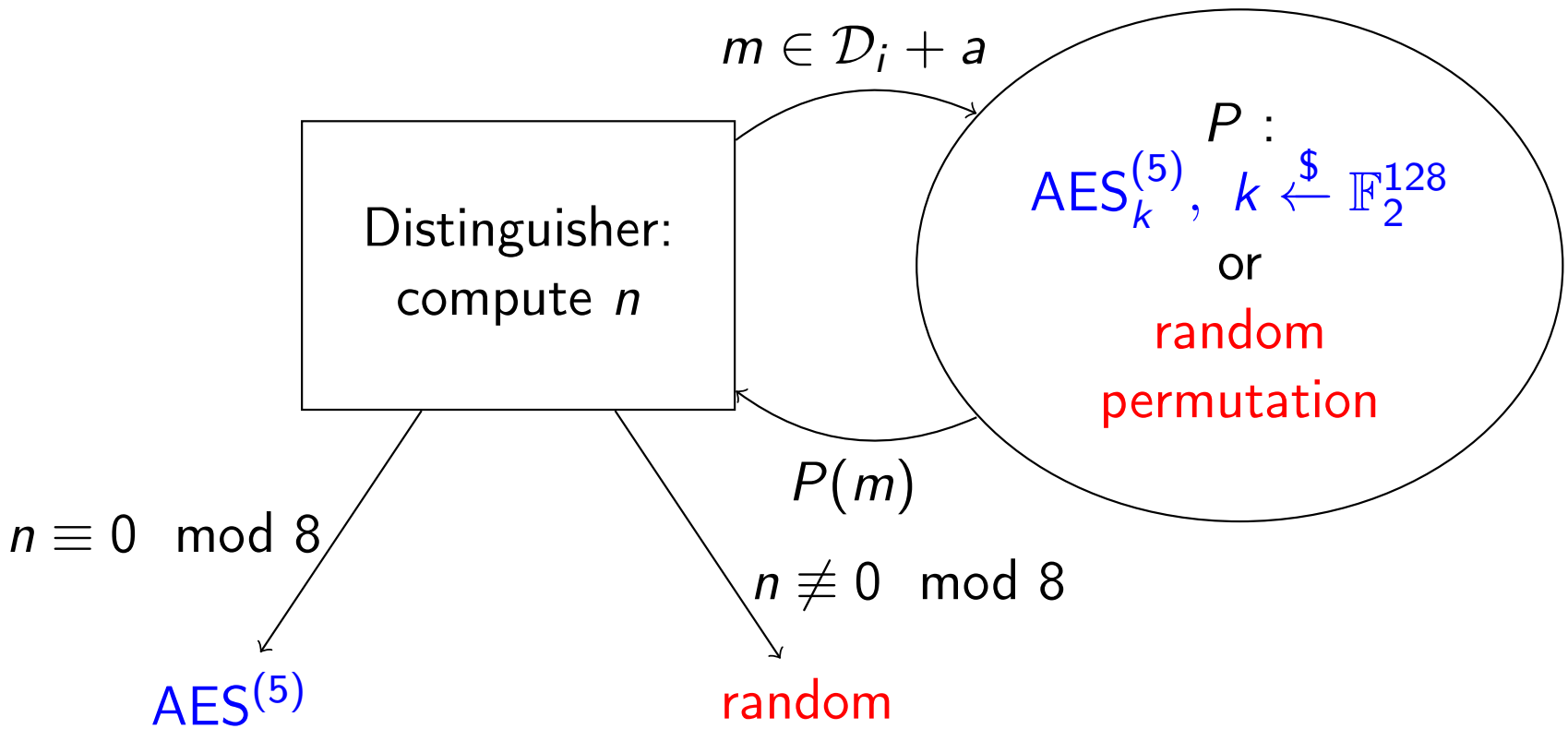
The distinguisher

Theorem ([GRR17])

Let $a \in \mathcal{M}_4(\mathbb{K})$, $i \in [\![0,3]\!]$, $J \subseteq [\![0,3]\!]$. *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 $n \equiv 0 \mod 8$.



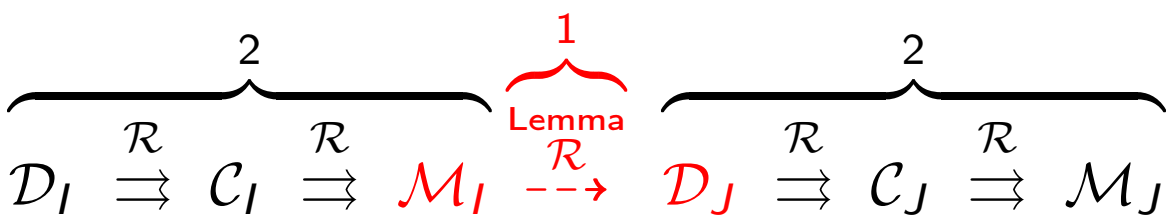
A key lemma

Lemma ([GRR17])

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

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

Then $n \equiv 0 \mod 8$.



Proof

In the original paper [GRR17]:

First case. First, we consider the case in which three variables are equ
W.l.o.g. we assume for example that $y = y'$, $z = z'$, $w = w'$ and $x \neq$
(the other cases are analogous). In other words, we suppose that the two te
p^1 and p^2 belong to the same coset of $\mathcal{M}_0 \cap \mathcal{C}_0 \oplus a$, where $a \in (\mathcal{M}_0 \cap \mathcal{C}_0)^{\perp}$.

Since $\mathcal{M}_0 \cap \mathcal{C}_0 \subseteq \mathcal{C}_0$, it follows that if $p^1 \oplus p^2 \in \mathcal{C}_0$, then $R(p^1) \oplus R(p^2) \in \mathcal{M}$
Since $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$ for each I and J with $|I|+|J| \leq 4$ (see (3)), it follows th
$R(p^1) \oplus R(p^2) \notin \mathcal{D}_J$ for each $J \subseteq \{0,1,2,3\}$ with $|J| \leq 3$. In other words, w
the given hypothesis for this case, it is not possible that the two texts belong
the same coset of a diagonal space $\mathcal{D}_J$ for each $|J| \leq 3$ after one round.

For completeness, it is also possible to show the same result in a differ
way. By definition, $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for a certain J with $|J| = 3$ if and o
if $(R(p^1) \oplus R(p^2))_{i,j+i} = 0$ for each $i = 0, ..., 3$ (i.e. the four bytes of the j
diagonal of $R(p^1) \oplus R(p^2)$ are equal to zero), where the indexes are taken mod
4 and $j = \{0,1,2,3\} \setminus J$. As we are going to show, due to the given hypothe
of this case and since the branch number of the MixColumns operation is eq
to five, it follows that $R(p^1) \oplus R(p^2) \notin \mathcal{D}_J$ for all J with $|J| = 3$. In other wo
$R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for $|J| = 3$ if and only if $x = x'$, that is $p^1 = p^2$.

In more details, by simple computation the first column (analogues for
other ones) of $SR \circ$ S-Box$(p^1) \oplus SR \circ$ S-Box(p^2) - denoted by $(SR \circ$ S-Box$(p^1$
$SR \circ$ S-Box$(p^2))_{,0}$ - is equal to:

$$(SR \circ \text{S-Box}(p^1) \oplus SR \circ \text{S-Box}(p^2))_{,0} = \begin{bmatrix} \text{S-Box}(2 \cdot x \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x' \oplus \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

After the MixColumns operation (note $R(p^1) \oplus R(p^2) = MC(SR \circ$ S-Box$(p^1$
$SR \circ$ S-Box$(p^2))$ = $MC \circ SR \circ$ S-Box$(p^1) \oplus MC \circ SR \circ$ S-Box$(p^2))$, since o
one input byte[10] is different from zero, it follows that at least four output by
must be different from zero, that is all the output bytes are different from ze
This simply implies that it is not possible that $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for $|J| \leq$

Second case. Secondly, we consider the case in which two variables are equ
that is w.l.o.g. we assume for example that $z = z'$ and $w = w'$, while $x \neq x'$ a
$y \neq y'$ (the other cases are analogous). That is, we suppose that the two te
p^1 and p^2 belong to the same coset of $\mathcal{M}_0 \cap \mathcal{C}_{0,1} \oplus a$, where $a \in (\mathcal{M}_0 \cap \mathcal{C}_{0,1})$

Assume that - for certain $z = z'$ and $w = w'$ - there exist two elements
(generated by $\langle x, y \rangle$) and p^2 (generated by $\langle x', y' \rangle$) defined as before in the sa
coset of $\mathcal{M}_0$ that belong to the same coset of $\mathcal{D}_J$ for a certain J with $|J| =$
after one round. In other words, let $j = \{0,1,2,3\} \setminus J$ and assume that th
exist x, y and x', y' and j such that the generated elements p^1 and p^2 sati
$(R(p^1) \oplus R(p^2))_{i,i+j} = 0$ for each $i = 0,1,2,3$, where the indexes are tal
modulo 4.

[10] Note that S-Box$(2 \cdot x \oplus a_{0,0}) \oplus$ S-Box$(2 \cdot x' \oplus a_{0,0}) = 0$ if and only if $x = x'$, wh
can never happen for hypothesis.

This implies that the two elements $\bar{p}^1$ (generated by $\langle x, y' \rangle$) and $\bar{p}^2$ (genera
by $\langle x, y' \rangle$)

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

belong to the same coset of $\mathcal{D}_J$ after one round. To prove this fact, it is sufficie
to compute $R(p^1) \oplus R(p^2)$ and $R(\bar{p}^1) \oplus R(\bar{p}^2)$, and to prove that they are eq
i.e.

$$R(p^1) \oplus R(p^2) = R(\bar{p}^1) \oplus R(\bar{p}^2).$$

Since $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$, it also follows that $R(\bar{p}^1) \oplus R(\bar{p}^2) \in \mathcal{D}_J$. In particu
by simple computation the first column of $R(p^1) \oplus R(p^2)$ is given by:

$$\begin{aligned}
(R(p^1) \oplus R(p^2))_{0,0} &= 2 \cdot (\text{S-Box}(2 \cdot x \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x' \oplus a_{0,0})) \oplus \\
&\quad \oplus 3 \cdot (\text{S-Box}(y \oplus a_{1,1}) \oplus \text{S-Box}(y' \oplus a_{1,1})), \\
(R(p^1) \oplus R(p^2))_{1,0} &= \text{S-Box}(2 \cdot x \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x' \oplus a_{0,0}) \oplus \\
&\quad \oplus 2 \cdot (\text{S-Box}(y \oplus a_{1,1}) \oplus \text{S-Box}(y' \oplus a_{1,1})), \\
(R(p^1) \oplus R(p^2))_{2,0} &= \text{S-Box}(2 \cdot x \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x' \oplus a_{0,0}) \oplus \\
&\quad \oplus \text{S-Box}(y \oplus a_{1,1}) \oplus \text{S-Box}(y' \oplus a_{1,1}), \\
(R(p^1) \oplus R(p^2))_{3,0} &= 3 \cdot (\text{S-Box}(2 \cdot x \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x' \oplus a_{0,0})) \oplus \\
&\quad \oplus \text{S-Box}(y \oplus a_{1,1}) \oplus \text{S-Box}(y' \oplus a_{1,1}).
\end{aligned}$$

Due to the definition of $\bar{p}^1$ and $\bar{p}^2$, it follows immediately that $(R(p^1) \oplus R(p^2))_{,}$
$(R(\bar{p}^1) \oplus R(\bar{p}^2))_{,0}$. The same holds for the other columns. Note that the existe
of the two elements $\bar{p}^1$ and $\bar{p}^2$ is guaranteed by the fact that we are working w
the entire coset of $\mathcal{M}_0$. This implies that the number of collisions must be ev
that is a multiple of 2.

Question: given p^1 and p^2 as before, is it possible that x, y, x', y' exist s
that $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for $|J| = 3$? Yes, again because the branch num
of the MixColumns operation is five. Indeed, compute $SR \circ$ S-Box$(p^1) \oplus S$
S-Box(p^2) and analyze the first column (the others are analogous):

$$(SR \circ \text{S-Box}(p^1) \oplus SR \circ \text{S-Box}(p^2))_{,0} = \begin{bmatrix} \text{S-Box}(2 \cdot x \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x' \oplus \\ \text{S-Box}(y \oplus a_{1,1}) \oplus \text{S-Box}(y' \oplus a_{1,1} \\ 0 \\ 0 \end{bmatrix}$$

After the MixColumns operation (note $R(p^1) \oplus R(p^2) = MC(SR \circ$ S-Box$(p^1$
$SR \circ$ S-Box$(p^2))$), since two input bytes[11] are different from zero, it follows t

[11] Note that S-Box$(2 \cdot x \oplus a_{0,0}) \oplus$ S-Box$(2 \cdot x' \oplus a_{0,0}) = 0$ if and only if $x = x'$, which
never happen for hypothesis. In the same way, S-Box$(y \oplus a_{1,1}) \oplus$ S-Box$(y' \oplus a_{1,1})$
if and only if $y = y'$, which can never happen for hypothesis.

at least three output bytes must be different from zero, or at most one out
byte could be equal to zero (similar for the other columns). In other words, i
possible that p^1 and p^2 exist such that $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for $|J| = 3$. Moreo
this also implies that it is not possible that two or more output bytes in the sa
column are equal to zero, or in other words that $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for $|J| \leq$
with the previous conditions.

Moreover, observe that $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for $|J| = 3$ if and only if t
bytes (one per column) of $R(p^1) \oplus R(p^2)$ are equal to zero. Since there are f
"free" variables (i.e. x, y, x', y') and a system of four equations, such a syst
can have a non-negligible solution.

Finally, since the previous result is independent of the values of $z = z'$ a
$w = w'$, it follows that the number of collisions for this case must be a multi
of 2^{17}. Indeed, assume that for certain $\bar{z}$ and $\bar{w}$ there exist x, y, x', y' such t
the two elements p^1 and p^2 in $\mathcal{M}_0 \cap \mathcal{C}_{0,1} \oplus a$ generated respectively by $\langle x
and by $\langle x', y' \rangle$ satisfy the condition $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for a certain J.
simple computation, the difference $R(p^1) \oplus R(p^2)$ doesn't depend on $z = z'$ a
on $w = w'$, that is for each byte of $(R(p^1) \oplus R(p^2))_{k,l}$ for $k, l = 0, 1, 2, 3$ th
exist constant A_i, B_i, C_i for $i = 0, 1, 2, 3$ - that depend only on the coefficie
of the MixColumns matrix or/and of the secret-key - such that

$$\begin{aligned}
(R(p^1) \oplus R(p^2))_{i,j} &= A_0 \cdot (\text{S-Box}(B_0 \cdot x \oplus C_0) \oplus \text{S-Box}(B_0 \cdot x' \oplus C_0)) \oplus \\
&\quad \oplus A_1 \cdot (\text{S-Box}(B_1 \cdot y \oplus C_1) \oplus \text{S-Box}(B_1 \cdot y' \oplus C_1)) \oplus \\
&\quad \oplus A_2 \cdot (\text{S-Box}(B_2 \cdot z \oplus C_2) \oplus \text{S-Box}(B_2 \cdot z' \oplus C_2)) \oplus \\
&\quad \oplus A_3 \cdot (\text{S-Box}(B_3 \cdot w \oplus C_3) \oplus \text{S-Box}(B_3 \cdot w' \oplus C_3)) = \\
&= A_0 \cdot (\text{S-Box}(B_0 \cdot x \oplus C_0) \oplus \text{S-Box}(B_0 \cdot x' \oplus C_0)) \oplus \\
&\quad \oplus A_1 \cdot (\text{S-Box}(B_1 \cdot y \oplus C_1) \oplus \text{S-Box}(B_1 \cdot y' \oplus C_1)).
\end{aligned}$$

It follows that - under the previous hypothesis - each pair of elements p^1 and
respectively generated by (1) $\langle x, y, z, w \rangle$ and by $\langle x', y', z, w \rangle$ or (2) $\langle x, y', z,$
and by $\langle x', y, z, w \rangle$ *for each possible value of* z *and* w satisfy the condition $R(p^1$
$R(p^2) \in \mathcal{D}_J$. Thus, the number of collisions for this case must be a multipl
$2 \cdot (2^8)^2 = 2^{17}$. As before, the existence of all these elements is guaranteed
the fact that we are working with the entire coset of $\mathcal{M}_0$.

Third case. Thirdly, we consider the case in which only one variable is equ
that is w.l.o.g. we assume for example $w = w'$, while $x \neq x'$, $y \neq y'$ and $z \neq$
(the other cases are analogous). That is, we suppose that the two texts p^1 a
p^2 belong to the same coset of $\mathcal{M}_0 \cap \mathcal{C}_{0,1,2} \oplus a$, where $a \in (\mathcal{M}_0 \cap \mathcal{C}_{0,1,2})^{\perp}$.

Assume there exist two elements p^1 (generated by $\langle x, y, z \rangle$) and p^2 (genera
by $\langle x', y', z' \rangle$) defined as before in the same coset of $\mathcal{M}_0$ that belong to the sa
coset of $\mathcal{D}_J$ for a certain J with $|J| \geq 2$ after one round. In other words, assu
there exist x, y, z and x', y', z' such that the generated elements p^1 and p^2 sat
$R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for a certain J with $|J| \geq 2$ Similar to before, it follows t
also the following three pairs of elements in the same coset of $\mathcal{M}_0$ generated

- $\langle x', y, z \rangle$ and $\langle x, y', z' \rangle$
- $\langle x, y', z \rangle$ and $\langle x', y, z' \rangle$
- $\langle x, y, z' \rangle$ and $\langle x', y', z \rangle$

belong after one round in the same coset of $\mathcal{D}_J$ for the same J of p^1 and p^2,
a total of four different pairs. As before, in order to prove this fact it is suffici
to show that $R(p^1) \oplus R(p^2) = R(\bar{p}^1) \oplus R(\bar{p}^2)$, where $\bar{p}^1$ and $\bar{p}^2$ are generated
the previous combinations of variables. Note that the existence of these eleme
is guaranteed by the fact that we are working with the entire coset of $\mathcal{M}_0$. T
implies that the number of collisions must be a multiple of 4.

Finally, we have only to prove that such x, y, z and x', y', z' can exist.
before, we compute $SR \circ$ S-Box$(p^1) \oplus SR \circ$ S-Box(p^2) and analyze the first colu
(the others are analogous):

$$(SR \circ \text{S-Box}(p^1) \oplus SR \circ \text{S-Box}(p^2))_{,0} = \begin{bmatrix} \text{S-Box}(2 \cdot x \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x' \oplus \\ \text{S-Box}(y \oplus a_{1,1}) \oplus \text{S-Box}(y' \oplus a_{1,1} \\ \text{S-Box}(2 \cdot z \oplus a_{2,2}) \oplus \text{S-Box}(2 \cdot z' \oplus \\ 0 \end{bmatrix}$$

After the MixColumns operation, since three input bytes[12] are different fr
zero, it follows that at least two output bytes must be different from zero.
at most two output bytes could be equal to zero. This implies that the ev
$R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for $|J| \geq 2$ is possible. Moreover, this also implies that i
not possible that three output bytes (of the same column) are equal to zero, o
other words that $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for $|J| = 1$, with the previous hypothe
Also in this case, variables x, y, z and x', y', z' can exist since the number
equations is less or equal than the number of variables.

Finally, since the previous result is independent of the values of $w = w'$
follows that the number of collisions for this case must be a multiple of $4 \cdot 2^8 =$
As before, assume that for a certain $\bar{w}$ there exist x, y, z, x', y', z' such that
two elements p^1 and p^2 in $\mathcal{M}_0 \cap \mathcal{C}_{0,1,2} \oplus a$ generated respectively by $\langle x, y, z \rangle$
by $\langle x', y', z' \rangle$ satisfy the condition $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for a certain J. Also
this case, the idea is to show that the difference $R(p^1) \oplus R(p^2)$ doesn't depend
$w = w'$, that is for each byte of $(R(p^1) \oplus R(p^2))_{i,j}$ there exist constant A_i, B_i
for $i = 0, 1, 2$ - that depend only on the coefficients of the MixColumns mat
or/and of the secret-key - such that

$$\begin{aligned}
(R(p^1) \oplus R(p^2))_{i,j} &= A_0 \cdot (\text{S-Box}(B_0 \cdot x \oplus C_0) \oplus \text{S-Box}(B_0 \cdot x' \oplus C_0)) \oplus \\
&\quad \oplus A_1 \cdot (\text{S-Box}(B_1 \cdot y \oplus C_1) \oplus \text{S-Box}(B_1 \cdot y' \oplus C_1)) \oplus \\
&\quad \oplus A_2 \cdot (\text{S-Box}(B_2 \cdot z \oplus C_2) \oplus \text{S-Box}(B_2 \cdot z' \oplus C_2)).
\end{aligned}$$

It follows that - under the previous hypothesis - each pair of elements p^1 and
respectively generated by one of the four different combinations of the varial

[12] Note that S-Box$(2 \cdot x \oplus a_{0,0}) \oplus$S-Box$(2 \cdot x' \oplus a_{0,0}) =$ S-Box$(y \oplus a_{1,1}) \oplus$S-Box$(y' \oplus a_{1,1}$
S-Box$(2 \cdot z \oplus a_{2,2}) \oplus$ S-Box$(2 \cdot z' \oplus a_{2,2}) = 0$ if and only if $x = x'$, $y = y'$ and $z =$
which can never happen for hypothesis.

$\langle x, y, z, w \rangle$ and $\langle x', y', z', w \rangle$ *for each possible value of* w satisfy the condit
different, that is w.l.o.g. we assume that $x \neq x'$, $y \neq y'$, $z \neq z'$ and $w \neq$
That is, we suppose that the two texts p^1 and p^2 belong to the same coset
$\mathcal{M}_0 \oplus a$, where $a \in \mathcal{M}_0^{\perp}$ and where $p^1 \oplus p^2 \notin \mathcal{C}_J$ for each $|J| \leq 3$.

Assume there exist two elements p^1 (generated by $\langle x, y, z, w \rangle$) and p^2 (g
erated by $\langle x', y', z', w' \rangle$) defined as before in the same coset of $\mathcal{M}_0$ that bel
to the same coset of $\mathcal{D}_J$ for a certain J with $|J| \geq 1$ after one round. In ot
words, assume there exist x, y, z, w and x', y', z', w' such that the generated
ments p^1 and p^2 satisfy $R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for a certain J with $|J| \geq 1$. Sim
to before, it follows that also the following seven pairs of elements in the sa
coset of $\mathcal{M}_0$ generated by:

- $\langle x', y, z, w \rangle$ and $\langle x, y', z', w' \rangle$
- $\langle x, y', z, w \rangle$ and $\langle x', y, z', w' \rangle$
- $\langle x, y, z', w \rangle$ and $\langle x', y', z, w' \rangle$
- $\langle x, y, z, w' \rangle$ and $\langle x', y', z', w \rangle$
- $\langle x', y', z, w \rangle$ and $\langle x, y, z', w' \rangle$
- $\langle x', y, z', w \rangle$ and $\langle x, y', z, w' \rangle$
- $\langle x', y, z, w' \rangle$ and $\langle x, y', z', w \rangle$

belong after one round in the same coset of $\mathcal{D}_J$ for the same J of p^1 and
for a total of eight different pairs. As before, in order to prove this fact it
sufficient to show that $R(p^1) \oplus R(p^2) = R(\bar{p}^1) \oplus R(\bar{p}^2)$. Moreover, as before n
that existence of these elements is guaranteed by the fact that we are work
with all the coset of $\mathcal{M}_0$. This implies that the number of collisions must b
multiple of 8.

Finally, we have only to prove that such x, y, z, w and x', y', z', w' can ex
As before, we compute $SR \circ$ S-Box$(p^1) \oplus SR \circ$ S-Box(p^2) and analyze the f
column (the others are analogous):

$$(SR \circ \text{S-Box}(p^1) \oplus SR \circ \text{S-Box}(p^2))_{,0} = \begin{bmatrix} \text{S-Box}(2 \cdot x \oplus a_{0,0}) \oplus \text{S-Box}(2 \cdot x' \oplus \\ \text{S-Box}(y \oplus a_{1,1}) \oplus \text{S-Box}(y' \oplus a_{1,1} \\ \text{S-Box}(2 \cdot z \oplus a_{2,2}) \oplus \text{S-Box}(2 \cdot z' \oplus \\ \text{S-Box}(w \oplus a_{3,3}) \oplus \text{S-Box}(w' \oplus a_{3,} \end{bmatrix}$$

After the MixColumns operation, since four input bytes[13] are different fr
zero, it follows that at least one output byte must be different from zero,
at most three output bytes could be equal to zero. This implies that the ev
$R(p^1) \oplus R(p^2) \in \mathcal{D}_J$ for $|J| \geq 1$ is possible. Also in this case, variables x, y, z
and x', y', z', w' can exist since the number of equations is less or equal than
number of variables.

[13] Note that S-Box$(2 \cdot x \oplus a_{0,0}) \oplus$S-Box$(2 \cdot x' \oplus a_{0,0}) =$ S-Box$(y \oplus a_{1,1}) \oplus$S-Box$(y' \oplus a_{1,1}$
S-Box$(2 \cdot z \oplus a_{2,2}) \oplus$S-Box$(2 \cdot z' \oplus a_{2,2}) =$ S-Box$(w \oplus a_{3,3}) \oplus$S-Box$(w' \oplus a_{3,3}) = 0$ if
only if $x = x'$, $y = y'$, $z = z'$ and $w = w'$, which can never happen for hypothesi

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 $\mathcal{M}_0$,

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

$$\sim$$

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

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

$$\sim$$

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

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.

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

$$\sim$$

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

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.
- $\forall k \in K, \exists b \in \{0,1\} : \forall i \in I, q^0_{i,k} = p^b_{i,k}$ et $q^1_{i,k} = p^{1-b}_{i,k}$.

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

Lemma

The function

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

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

Proposition

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

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

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 $n \equiv 0 \mod 8$.

Proof.

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

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

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

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 $n \equiv 0 \mod 8$.

Proof.

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

Definition

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

$$\begin{pmatrix}
* & \cdots & * & & & & & & \\
\vdots & \lambda_{0,\ell,i} & \vdots & & 0 & & & 0 & \\
* & \cdots & * & & & & & & \\
 & & & * & \cdots & * & & & \\
 & 0 & & \vdots & \lambda_{k,\ell,i} & \vdots & & 0 & \\
 & & & * & \cdots & * & & & \\
 & & & & & & * & \cdots & * \\
 & 0 & & & 0 & & \vdots & \lambda_{h-1,\ell,i} & \vdots \\
 & & & & & & * & \cdots & * \\
 & 0 & & & 0 & & & 0 & \\
 & \uparrow & & & \uparrow & & & \uparrow & \\
 & g_{0,i} & & & g_{k,i} & & & g_{h-1,i} &
\end{pmatrix}$$

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

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

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

Midori

Midori, presented at Asiacrypt 2015 [BBI+15].
Goal: low energy consumption.

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

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

$$\overbrace{\mathcal{D}'_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{C}_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{M}'_I}^{2} \quad \overbrace{\overset{\mathcal{R}}{\dashrightarrow}}^{1} \text{ Genaralized Lemma} \quad \overbrace{\mathcal{D}'_J \overset{\mathcal{R}}{\rightrightarrows} \mathcal{C}_J \overset{\mathcal{R}}{\rightrightarrows} \mathcal{M}'_J}^{2}$$

What now ?

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

$$\overbrace{\mathcal{D}'_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{C}_I \overset{\mathcal{R}}{\rightrightarrows} \mathcal{M}'_I}^{2} \overbrace{\underset{\text{Genaralized Lemma}}{\overset{\mathcal{R}}{\dashrightarrow}}}^{1} \overbrace{\mathcal{D}'_J \overset{\mathcal{R}}{\rightrightarrows} \mathcal{C}_J \overset{\mathcal{R}}{\rightrightarrows} \mathcal{M}'_J}^{2}$$


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.