A General Proof Framework for Recent AES Distinguishers

Christina Boura, Anne Canteaut, Daniel Coggia

Inria, Project Team SECRET, France

March 27, FSE 2019

Outline

Definitions and the multiple-of-8 distinguisher

Proof for the distinguisher

Generalisation of this proof framework

Adaptation to other SPN ciphers

Some definitions...

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

Some definitions...

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

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

Columns

Some definitions...

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

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

Columns

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

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

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

Diagonals

$$\mathcal{D}_I \xrightarrow{\texttt{ShiftRows}} \mathcal{C}_I$$

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

Diagonals

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

Anti-diagonals

$$\mathcal{C}_I \xrightarrow{\texttt{ShiftRows}} \mathcal{ID}_I$$

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

Diagonals

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

Anti-diagonals

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

Mixed

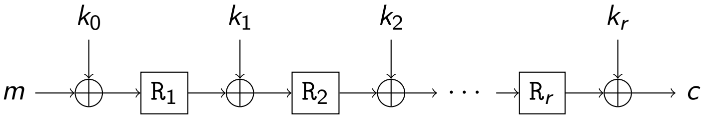
$$\mathcal{ID}_I \xrightarrow{\texttt{MixColumns}} \mathcal{M}_I$$

$$\color{red}{\mathcal{D}_I}\ \overbrace{\xrightarrow{\texttt{SubBytes}} \mathcal{D}_I \xrightarrow{\texttt{ShiftRows}} \mathcal{C}_I \xrightarrow{\texttt{MixColumns}}}^{\texttt{R}}\ \color{red}{\mathcal{C}_I}$$

$$\color{red}{\mathcal{C}_I}\ \overbrace{\xrightarrow{\texttt{SubBytes}} \mathcal{C}_I \xrightarrow{\texttt{ShiftRows}} \mathcal{ID}_I \xrightarrow{\texttt{MixColumns}}}^{\texttt{R}}\ \color{red}{\mathcal{M}_I}$$

$$\mathcal{D}_I \overbrace{\xrightarrow{\texttt{SubBytes}} \mathcal{D}_I \xrightarrow{\texttt{ShiftRows}} \mathcal{C}_I \xrightarrow{\texttt{MixColumns}}}^{\texttt{R}} \mathcal{C}_I$$

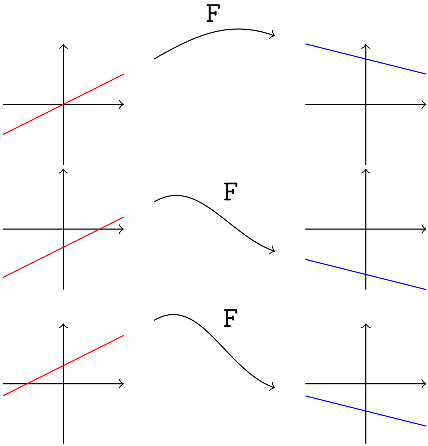
$$\mathcal{C}_I \overbrace{\xrightarrow{\texttt{SubBytes}} \mathcal{C}_I \xrightarrow{\texttt{ShiftRows}} \mathcal{ID}_I \xrightarrow{\texttt{MixColumns}}}^{\texttt{R}} \mathcal{M}_I$$



Subspace trails

Grassi, Rechberger and Rønjom, ToSC 2016

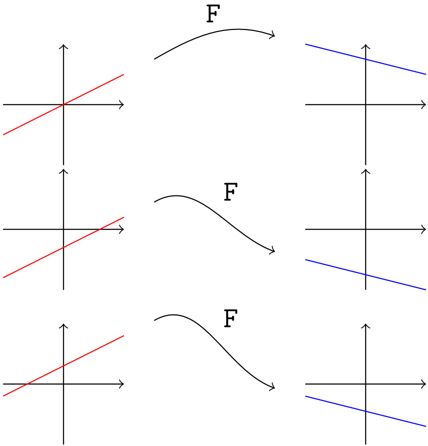
$$\mathcal{U} \overset{\mathtt{F}}{\rightrightarrows} \mathcal{V} \qquad \text{if} \qquad \forall a \in \mathbb{F}_{2^8}^{16},\ \exists b \in \mathbb{F}_{2^8}^{16} :\ \mathtt{F}(\mathcal{U} + a) = \mathcal{V} + b.$$



Subspace trails

Grassi, Rechberger and Rønjom, ToSC 2016

$$\mathcal{U} \overset{\texttt{F}}{\rightrightarrows} \mathcal{V} \qquad \text{if} \qquad \forall a \in \mathbb{F}_{2^8}^{16},\ \exists b \in \mathbb{F}_{2^8}^{16} :\ \texttt{F}(\mathcal{U} + a) = \mathcal{V} + b.$$



Examples:

- $\{0\} \overset{\texttt{F}}{\rightrightarrows} \{0\}$
- $U \overset{\texttt{F}}{\rightrightarrows} \mathbb{F}_{2^8}^{N}$
- $\mathcal{D}_I \overset{\texttt{R}}{\rightrightarrows} \mathcal{C}_I$
- $\mathcal{C}_I \overset{\texttt{R}}{\rightrightarrows} \mathcal{M}_I$

The multiple-of-8 distinguisher

Grassi, Rechberger and Rønjom, Eurocrypt 2017

$a \in \mathbb{F}_{2^8}^{16}$

The multiple-of-8 distinguisher

Grassi, Rechberger and Rønjom, Eurocrypt 2017

$a \in \mathbb{F}_{2^8}^{16}$ $\quad\quad$ $i \in \{0, \ldots, 3\} : \mathcal{D}_i$

The multiple-of-8 distinguisher

Grassi, Rechberger and Rønjom, Eurocrypt 2017

$a \in \mathbb{F}_{2^8}^{16}$ $\quad i \in \{0, \ldots, 3\} : \mathcal{D}_i$ $\quad J \subseteq \{0, \ldots, 3\} : \mathcal{M}_J$

The multiple-of-8 distinguisher

Grassi, Rechberger and Rønjom, Eurocrypt 2017

$a \in \mathbb{F}_{2^8}^{16}$ $\quad i \in \{0, \ldots, 3\} : \mathcal{D}_i$ $\quad J \subseteq \{0, \ldots, 3\} : \mathcal{M}_J$

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

The multiple-of-8 distinguisher

Grassi, Rechberger and Rønjom, Eurocrypt 2017

$a \in \mathbb{F}_{2^8}^{16}$ $\qquad i \in \{0, \ldots, 3\} : \mathcal{D}_i$ $\qquad J \subseteq \{0, \ldots, 3\} : \mathcal{M}_J$

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

Then $n \equiv 0 \mod 8$.

Our contribution starts here

Questions to answer:

- Is the maximal branch number necessary ?
- Can we adapt this distinguisher to other SPN ?

Our contribution starts here

Questions to answer:

- Is the maximal branch number necessary ? New proof
- Can we adapt this distinguisher to other SPN ?

Our contribution starts here

Questions to answer:

- Is the maximal branch number necessary ? New proof
- Can we adapt this distinguisher to other SPN ? Adaptation of the new proof

Definitions and the multiple-of-8 distinguisher

Proof for the distinguisher

Generalisation of this proof framework

Adaptation to other SPN ciphers

A key lemma

Grassi, Rechberger and Rønjom, Eurocrypt 2017

$$\overbrace{\mathcal{D}_I \overset{\texttt{R}}{\rightrightarrows} \mathcal{C}_I \overset{\texttt{R}}{\rightrightarrows} \mathcal{M}_I}^{2} \qquad \overbrace{\mathcal{D}_J \overset{\texttt{R}}{\rightrightarrows} \mathcal{C}_J \overset{\texttt{R}}{\rightrightarrows} \mathcal{M}_J}^{2}$$

A key lemma

Grassi, Rechberger and Rønjom, Eurocrypt 2017

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

A key lemma

Grassi, Rechberger and Rønjom, Eurocrypt 2017

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

Lemma

Let $a \in \mathbb{F}_{2^8}^{16}$, $I \subset [\![0,3]\!]$, $J \subseteq [\![0,3]\!]$. *We define*

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

Then $n \equiv 0 \mod 8$.

Step 1: equivalence relation between pairs

In $\mathcal{M}_0$

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

Definition

$p^0, p^1 \in (\mathcal{M}_I + a)$. The information set K of the pair $\{p^0, p^1\}$ is

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

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

$p^0, p^1, q^0, q^1 \in (\mathcal{M}_I + a), P = \{p^0, p^1\}, Q = \{q^0, q^1\}$

$P \sim Q$ if:

- P and Q share the same information set K.
- $\forall k \in K, \exists b \in \{0,1\} : \forall i \in I, q^0_{i,k} = p^b_{i,k}$ et $q^1_{i,k} = p^{1-b}_{i,k}$.

$\sim$ is an equivalence relation on the pairs of $(\mathcal{M}_I + a)$.

Theorem

The function

$$\Delta : \{p^0, p^1\} \longmapsto \mathtt{R}(p^0) + \mathtt{R}(p^1)$$

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

Theorem

The function

$$\Delta : \{p^0, p^1\} \longmapsto \mathtt{R}(p^0) + \mathtt{R}(p^1)$$

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

Proposition

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

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

Lemma

If

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

then $n \equiv 0 \mod 8$.

Proof.

$$\begin{aligned} n &= \#\Delta^{-1}(\mathcal{D}_J) \\ &= \sum_{\mathfrak{C}} \# \underbrace{(\Delta^{-1}(\mathcal{D}_J) \cap \mathfrak{C})}_{\varnothing \text{ or } \mathfrak{C}} \\ &\equiv 0 \mod 8 \end{aligned}$$

□

What about the branch number ?

With a proposition of Grassi, Rechberger and Rønjom, if b is the branch number,

$$
\begin{aligned}
n &= \#\Delta^{-1}(\mathcal{D}_J) \\
&= \sum_{\mathfrak{C}} \#(\Delta^{-1}(\mathcal{D}_J) \cap \mathfrak{C}) \\
&= \sum_{\mathfrak{C}:\ |K(\mathfrak{C})| \geq b - |J|} \# \underbrace{(\Delta^{-1}(\mathcal{D}_J) \cap \mathfrak{C})}_{\varnothing \text{ or } \mathfrak{C}} \\
&\quad + \sum_{\mathfrak{C}:\ |K(\mathfrak{C})| < b - |J|} \# \underbrace{(\Delta^{-1}(\mathcal{D}_J) \cap \mathfrak{C})}_{\varnothing} \\
&\equiv 0 \mod 8
\end{aligned}
$$

First question answered

- Is the maximal branch number necessary ? No

- Can we adapt this distinguisher to other SPN ? Adaptation of the new proof

A few slides earlier...

$$\mathcal{C}_I \xrightarrow{\texttt{ShiftRows}} \mathcal{ID}_I \xrightarrow{\texttt{MixColumns}} \mathcal{M}_I$$

A few slides earlier...

$$\mathcal{C}_I \xrightarrow{\texttt{ShiftRows}} \mathcal{ID}_I \xrightarrow{\texttt{MixColumns}} \mathcal{M}_I$$

Definition

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

- P and Q share the same information set K.
- $\forall k \in K, \exists b \in \{0,1\} : \forall i \in I, q^0_{i,k} = p^b_{i,k}$ et $q^1_{i,k} = p^{1-b}_{i,k}$.

$\sim$ is an equivalence relation on the pairs of $(\mathcal{M}_I + a)$.

A few slides earlier...

$$\mathcal{C}_I \xrightarrow{\texttt{ShiftRows}} \mathcal{ID}_I \xrightarrow{\texttt{MixColumns}} \mathcal{M}_I$$

Definition

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

- P and Q share the same information set K.
- $\forall k \in K, \exists b \in \{0,1\} : \forall i \in I, q^0_{i,k} = p^b_{i,k}$ et $q^1_{i,k} = p^{1-b}_{i,k}$.

$\sim$ is an equivalence relation on the pairs of $(\mathcal{M}_I + a)$.

Theorem

The function

$$\Delta : \{p^0, p^1\} \longmapsto \mathtt{R}(p^0) + \mathtt{R}(p^1)$$

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

What relationship between
$\mathcal{M}_I$ and R makes it work ?

What relationship between $\mathcal{M}_I$ and `R` makes it work ?

Hint:
basis of $\mathcal{M}_{0,2}$ in the canonical basis (basis on which `SubBytes` is defined)

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

Basis g of $V \subseteq \mathbb{F}_{2^8}^{16}$ for which the theorem holds
i.e. V is compatible with `SubBytes`:

Basis g of $V \subseteq \mathbb{F}_{2^8}^{16}$ for which the theorem holds
i.e. V is compatible with `SubBytes`:

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

$$
\begin{matrix} \uparrow & \uparrow & \uparrow \\ g_{0,i} & g_{k,i} & g_{h-1,i} \end{matrix}
$$

Basis g of $V \subseteq \mathbb{F}_{2^8}^{16}$ for which the theorem holds
i.e. V is compatible with SubBytes: $\#\mathfrak{C} \equiv 0 \mod 2^{h-1}$

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

$$
\begin{matrix} \uparrow & \uparrow & \uparrow \\ g_{0,i} & g_{k,i} & g_{h-1,i} \end{matrix}
$$

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

$\mathcal{M}_0$ is compatible with `SubBytes`.

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

First mixture differential

Grassi, ToSC 2018

$$a \in \mathbb{F}_{2^8}^{16}$$

First mixture differential

Grassi, ToSC 2018

$a \in \mathbb{F}_{2^8}^{16}$ $U = \mathrm{vect}_{\mathbb{F}_{2^8}}(e_{0,1}, e_{1,1})$

First mixture differential

Grassi, ToSC 2018

$a \in \mathbb{F}_{2^8}^{16}$ $\qquad U = \mathrm{vect}_{\mathbb{F}_{2^8}}(e_{0,1}, e_{1,1}) \qquad J \subseteq \{0, 1, 2, 3\} : \mathcal{M}_J$

First mixture differential

Grassi, ToSC 2018

$a \in \mathbb{F}_{2^8}^{16}$ $\qquad U = \mathrm{vect}_{\mathbb{F}_{2^8}}(e_{0,1}, e_{1,1}) \qquad J \subseteq \{0,1,2,3\} : \mathcal{M}_J$

$$p^0, p^1, q^0, q^1 \in (U + a)$$

$$p^0 \equiv (x_0, x_1), \quad p^1 \equiv (y_0, y_1)$$

$$q^0 \equiv (x_0, y_1), \quad q^1 \equiv (y_0, x_1)$$

First mixture differential

Grassi, ToSC 2018

$a \in \mathbb{F}_{2^8}^{16}$ $\quad U = \mathrm{vect}_{\mathbb{F}_{2^8}}(e_{0,1}, e_{1,1})$ $\quad J \subseteq \{0, 1, 2, 3\} : \mathcal{M}_J$

$$p^0, p^1, q^0, q^1 \in (U + a)$$
$$p^0 \equiv (x_0, x_1), \quad p^1 \equiv (y_0, y_1)$$
$$q^0 \equiv (x_0, y_1), \quad q^1 \equiv (y_0, x_1)$$

Then

$$\mathtt{R}^4(p^0) + \mathtt{R}^4(p^1) \in \mathcal{M}_J \iff \mathtt{R}^4(q^0) + \mathtt{R}^4(q^1) \in \mathcal{M}_J.$$

Proof for the first mixture differential

$$U = \mathcal{C}_0 \cap \mathcal{D}_{0,1}$$

Proof for the first mixture differential

$$U = \mathcal{C}_0 \cap \mathcal{D}_{0,1} \qquad V = \mathcal{M}_0 \cap \mathcal{C}_{0,1}$$

Proof for the first mixture differential

$$U = \mathcal{C}_0 \cap \mathcal{D}_{0,1} \qquad V = \mathcal{M}_0 \cap \mathcal{C}_{0,1}$$

$$U \overset{\mathtt{R}}{\rightrightarrows} V$$

$$\exists b : \mathtt{R}(p^0), \mathtt{R}(p^1), \mathtt{R}(q^0), \mathtt{R}(q^1) \in (V + b)$$

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

V is compatible with `SubBytes`.

$$\begin{pmatrix} 2 \cdot x_0 & x_1 & 0 & 0 \\ x_0 & x_1 & 0 & 0 \\ x_0 & 3 \cdot x_1 & 0 & 0 \\ 3 \cdot x_0 & 2 \cdot x_1 & 0 & 0 \end{pmatrix} \in V.$$

An easy computation gives:

$$\mathtt{R}(p^0) \equiv (\mathtt{Sbox}(x_0 + a_{0,i}), \mathtt{Sbox}(x_1 + a_{1,i}))$$
$$\mathtt{R}(p^1) \equiv (\mathtt{Sbox}(y_0 + a_{0,i}), \mathtt{Sbox}(y_1 + a_{1,i}))$$

$$\mathtt{R}(q^0) \equiv (\mathtt{Sbox}(x_0 + a_{0,i}), \mathtt{Sbox}(y_1 + a_{1,i}))$$
$$\mathtt{R}(q^1) \equiv (\mathtt{Sbox}(y_0 + a_{0,i}), \mathtt{Sbox}(x_1 + a_{1,i}))$$

An easy computation gives:

$$\mathtt{R}(p^0) \equiv (\mathtt{Sbox}(x_0 + a_{0,i}), \mathtt{Sbox}(x_1 + a_{1,i}))$$
$$\mathtt{R}(p^1) \equiv (\mathtt{Sbox}(y_0 + a_{0,i}), \mathtt{Sbox}(y_1 + a_{1,i}))$$

$$\mathtt{R}(q^0) \equiv (\mathtt{Sbox}(x_0 + a_{0,i}), \mathtt{Sbox}(y_1 + a_{1,i}))$$
$$\mathtt{R}(q^1) \equiv (\mathtt{Sbox}(y_0 + a_{0,i}), \mathtt{Sbox}(x_1 + a_{1,i}))$$

$\{\mathtt{R}(p^0), \mathtt{R}(p^1)\} \sim \{\mathtt{R}(q^0), \mathtt{R}(q^1)\}$ in the compatible coset $(V + b)$

Theorem

The function

$$\Delta : \{r^0, r^1\} \longmapsto \mathtt{R}(r^0) + \mathtt{R}(r^1)$$

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

Theorem

The function

$$\Delta : \{r^0, r^1\} \longmapsto \mathtt{R}(r^0) + \mathtt{R}(r^1)$$

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

$$\Rightarrow \quad \mathtt{R}^2(p^0) + \mathtt{R}^2(p^1) = \mathtt{R}^2(q^0) + \mathtt{R}^2(q^1)$$

Theorem

The function

$$\Delta : \{r^0, r^1\} \longmapsto \mathtt{R}(r^0) + \mathtt{R}(r^1)$$

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

$$\Rightarrow \quad \mathtt{R}^2(p^0) + \mathtt{R}^2(p^1) = \mathtt{R}^2(q^0) + \mathtt{R}^2(q^1)$$

$$\text{Since } \mathcal{D}_J \overset{\mathtt{R}}{\rightrightarrows} \mathcal{C}_J \overset{\mathtt{R}}{\rightrightarrows} \mathcal{M}_J,$$

$$\mathtt{R}^4(p^0) + \mathtt{R}^4(p^1) \in \mathcal{M}_J \iff \mathtt{R}^4(q^0) + \mathtt{R}^4(q^1) \in \mathcal{M}_J.$$

Midori

Banik, Bogdanov, Isobe, Shibutani, Hiwatari, Akishita and Regazzoni at Asiacrypt 2015.

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

- `Sbox` : $\mathbb{F}_{2^d} \to \mathbb{F}_{2^d}$, $d = 4$ or $d = 8$
- `ShuffleCell SC` (`ShiftRows`-type permutation)
- `MixColumns` with branch number 4

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

Leander, Tezcan and Wiemer at ToSC 2018:

The longest subspace trails are of the form:

$$\mathcal{D}_I^{\mathsf{Mi}} \overset{\mathtt{R}}{\rightrightarrows} \mathcal{C}_I \overset{\mathtt{R}}{\rightrightarrows} \mathcal{M}_I^{\mathsf{Mi}}$$

A basis of $\mathcal{M}_0^{\mathsf{Mi}}$:

$$\begin{pmatrix}
0 & . & . & . \\
1 & . & . & . \\
1 & . & . & . \\
1 & . & . & . \\
. & 1 & . & . \\
. & 1 & . & . \\
. & 1 & . & . \\
. & 0 & . & . \\
. & . & 1 & . \\
. & . & 0 & . \\
. & . & 1 & . \\
. & . & 1 & . \\
. & . & . & 1 \\
. & . & . & 1 \\
. & . & . & 1 \\
. & . & . & 0
\end{pmatrix}$$

4 blocks $\Rightarrow \#\mathfrak{C} \equiv 0 \mod 8$.

Multiple-of-8 distinguisher on 5 (out of 16 or 20) rounds for Midori even if the branch number is 4:

$$\overbrace{\mathcal{D}_I^{\mathsf{Mi}} \overset{\mathtt{R}}{\rightrightarrows} \mathcal{C}_I \overset{\mathtt{R}}{\rightrightarrows} \mathcal{M}_I^{\mathsf{Mi}}}^{2} \quad \overbrace{\overset{\text{Adapted Lemma}}{\overset{\mathtt{R}}{\dashrightarrow}}}^{1} \quad \overbrace{\mathcal{D}_J^{\mathsf{Mi}} \overset{\mathtt{R}}{\rightrightarrows} \mathcal{C}_J \overset{\mathtt{R}}{\rightrightarrows} \mathcal{M}_J^{\mathsf{Mi}}}^{2}$$

$$\#\{\{p^0, p^1\} \text{ with } p^0, p^1 \in \mathcal{D}_i^{\mathsf{Mi}} + a \mid \mathtt{R}^5(p^0) + \mathtt{R}^5(p^1) \in \mathcal{M}_j^{\mathsf{Mi}}\} \equiv 0 \mod 8$$

Klein

Lightweight blockcipher proposed in 2011 by Gong, Nikova and Law.

$$\begin{pmatrix} x_0 & x_4 \\ x_1 & x_5 \\ x_2 & x_6 \\ x_3 & x_7 \end{pmatrix} \in \mathbb{F}_{2^8}^8$$

- $\mathtt{Sbox} : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ nibbles $\to \mathbb{F}_2^{64} = \mathbb{F}_{2^8}^4 \times \mathbb{F}_{2^8}^4$
- `RN`: `RotateNibbles`
- `MN`: `MixNibbles` applies the AES `MixColumns`

Leander, Tezcan and Wiemer at ToSC 2018:

Longest subspace trail:

$$\mathcal{D}_i^{\mathsf{KI}} \overset{\mathtt{R}}{\rightrightarrows} \mathcal{C}_i \overset{\mathtt{R}}{\rightrightarrows} \mathcal{M}_i^{\mathsf{KI}}$$

$\mathcal{M}_0^{\mathsf{KI}}$ basis:

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

2 blocks $\Rightarrow \#\mathfrak{C} \equiv 0 \mod 2$.

Multiple-of-2 distinguisher for 5 (out of 12, 16 or 20) rounds for Klein:

$$\overbrace{\mathcal{D}_i^{\mathsf{Kl}} \overset{\mathtt{R}}{\rightrightarrows} \mathcal{C}_i \overset{\mathtt{R}}{\rightrightarrows} \mathcal{M}_i^{\mathsf{Kl}}}^{2} \overbrace{\overset{\text{Adapted Lemma}}{\overset{\mathtt{R}}{\dashrightarrow}}}^{1} \overbrace{\mathcal{D}_j^{\mathsf{Kl}} \overset{\mathtt{R}}{\rightrightarrows} \mathcal{C}_j \overset{\mathtt{R}}{\rightrightarrows} \mathcal{M}_j^{\mathsf{Kl}}}^{2}$$

$$\#\{\{p^0, p^1\} \text{ with } p^0, p^1 \in \mathcal{D}_i^{\mathsf{Kl}} + a \mid \mathtt{R}^5(p^0) + \mathtt{R}^5(p^1) \in \mathcal{M}_j^{\mathsf{Kl}}\} \equiv 0 \mod 2$$

Conclusion

- Our generalised proof framework with algorithms of Leander, Tezcan and Wiemer can find:
  - mixture-differential distinguishers,
  - multiple-of properties.

  in a systematic way for any SPN.

Conclusion

- Our generalised proof framework with algorithms of Leander, Tezcan and Wiemer can find:
  - mixture-differential distinguishers,
  - multiple-of properties.

  in a systematic way for any SPN.

- Improvements highly limited by subspace trails

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