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].

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

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]

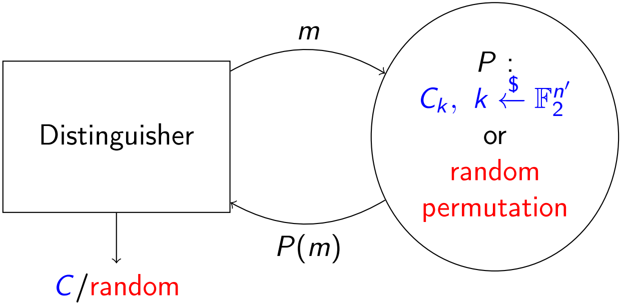
- The AES
- The distinguisher of Grassi, Rechberger and Rønjom

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...

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

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

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

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

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

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

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

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

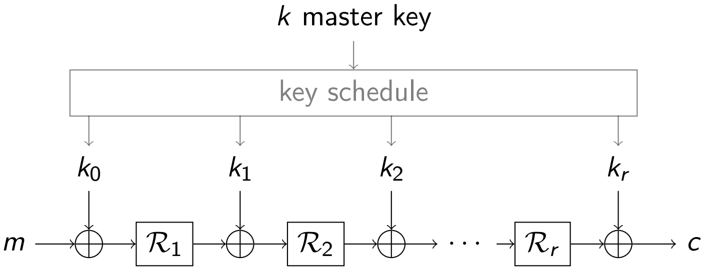
Anti-diagonals:
$\mathcal{ID}_i = SR(\mathcal{C}_i)$

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

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

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

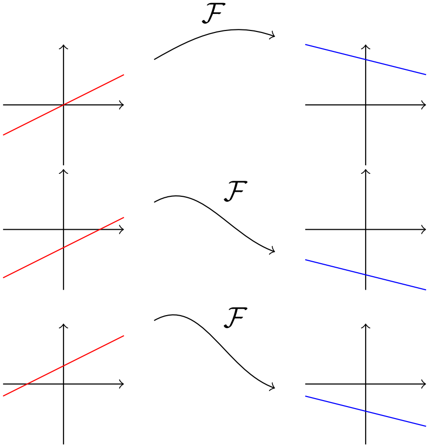
The AES is a key-alternating blockcipher



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:

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

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

$\forall a, \forall x,$

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

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

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

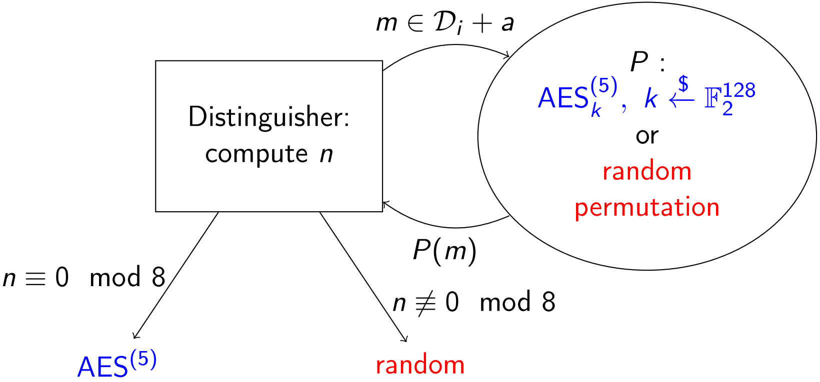
The distinguisher

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*

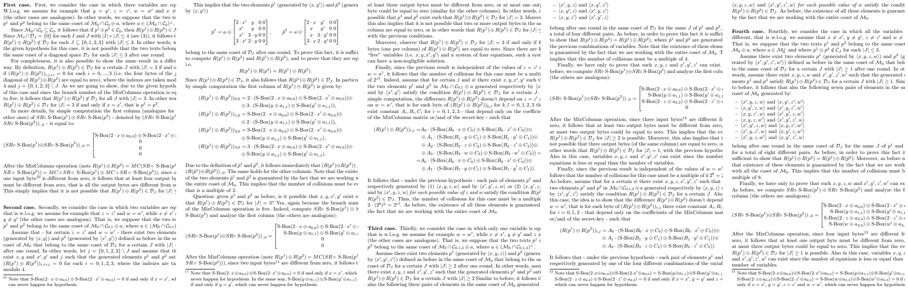
$$n = \#\{\ \{p^0, p^1\} \in \mathcal{P}^2(\mathcal{M}_I + a) \mid \mathcal{R}(p^0) + \mathcal{R}(p^1) \in \mathcal{D}_J \}.$$

Then $n \equiv 0 \mod 8$.

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

Proof

In the original paper [GRR17]:



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

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

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.

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

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

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

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:

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

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

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

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

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

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

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

What now ?

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

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

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.