Commutative Cryptanalysis Made Practical

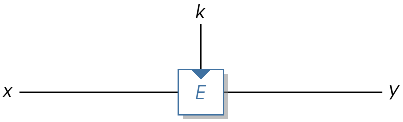
Jules Baudrin[1], Patrick Felke[2], Gregor Leander[3],
Patrick Neumann[3], Léo Perrin[1] & Lukas Stennes[3]

jules.baudrin@inria.fr

Inria

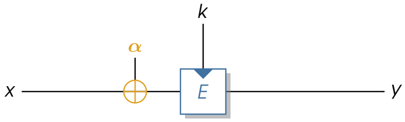
FSE, March 25th, 2024

1 Inria, Paris, France
2 University of Applied Sciences Emden/Leer, Emden, Germany
3 Ruhr University Bochum, Bochum, Germany

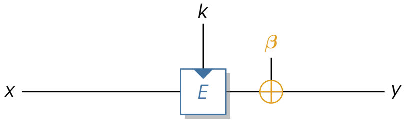

k
x
E
y

Observations on symmetric cryptanalysis

$$E(x + \alpha) = E(x) + \beta$$



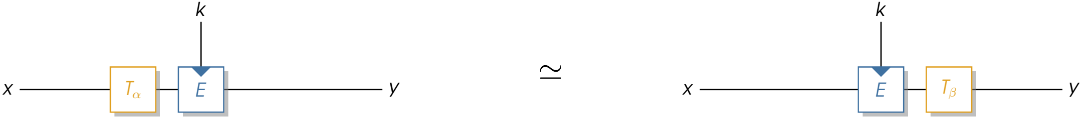
$\simeq$



Differential cryptanalysis

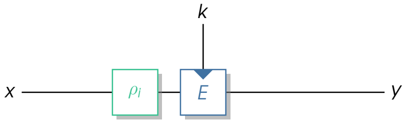
Observations on symmetric cryptanalysis

$$E \circ T_\alpha(x) = T_\beta \circ E(x)$$

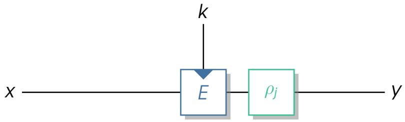


Differential cryptanalysis

$$E \circ \rho_i(x) = \rho_j \circ E(x)$$



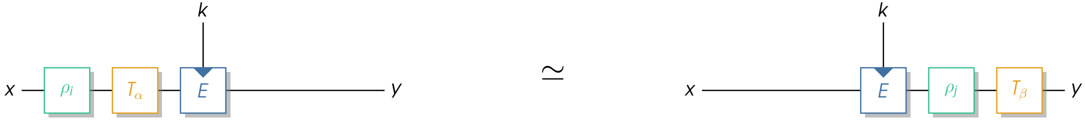
$$\simeq$$



Rotational cryptanalysis

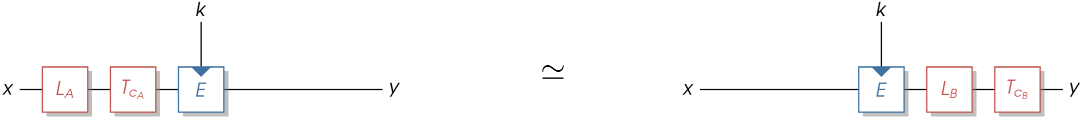
Observations on symmetric cryptanalysis

$$E \circ T_\alpha \circ \rho_i(x) = T_\beta \circ \rho_j \circ E(x)$$



Rotational-XOR cryptanalysis

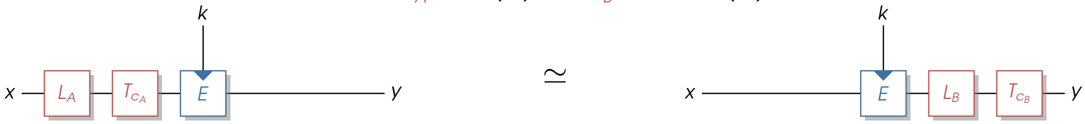
$$E \circ T_{c_A} \circ L_A(x) = T_{c_B} \circ L_B \circ E(x)$$



More general cryptanalysis ?

where $A(x) = L_A(x) + c_A, B(x) = L_B(x) + c_B$

$$E \circ T_{c_A} \circ L_A(x) = T_{c_B} \circ L_B \circ E(x)$$



More general cryptanalysis ?

where $A(x) = L_A(x) + c_A, B(x) = L_B(x) + c_B$

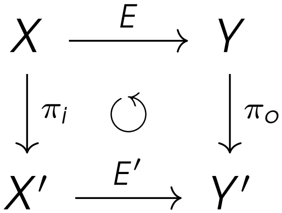
A tempting desire of unification

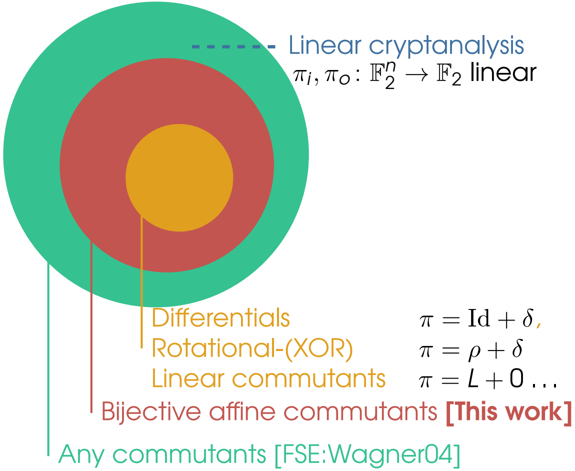
Mathematically elegant, better understanding, new attacks

A 20-year-old idea [Wagner, FSE 2004]

Commutative diagram cryptanalysis: not so fruitful[1] since.

[1] to the best of our knowledge...


$X \xrightarrow{E} Y$
π_i
π_o
$X' \xrightarrow{E'} Y'$


Linear cryptanalysis
$\pi_i, \pi_o : \mathbb{F}_2^n \to \mathbb{F}_2$ linear
Differentials $\pi = \mathrm{Id} + \delta$,
Rotational-(XOR) $\pi = \rho + \delta$
Linear commutants $\pi = L + 0 \ldots$
Bijective affine commutants **[This work]**
Any commutants [FSE:Wagner04]

In this talk

Affine commutation with **probability 1**: theory + practice

A **surprising differential** interpretation

A few words about the **probabilistic case**

Commutative cryptanalysis principle

Goal

Find **bijective affine** A, B st. for many k: $\boxed{E_k \circ A = B \circ E_k}$ (all x are solutions)

Commutative cryptanalysis principle

Goal

Find **bijective affine** A, B st. for many k: $\boxed{E_k \circ A = B \circ E_k}$ (all x are solutions)

$$E = R_{r-1} \circ \cdots \circ R_1 \circ R_0$$

Goal

Find **bijective affine** A, B st. for many k: $\boxed{E_k \circ A = B \circ E_k}$ (all x are solutions)

$$E = R_{r-1} \circ \cdots \circ R_1 \circ R_0$$

Sufficient condition for **iterated** constructions

There exist $A_0, \cdots, A_r$ st. for all i $\boxed{A_{i+1} \circ R_i = R_i \circ A_i}$.

$$\begin{array}{ccccccc}
x_0 & \xrightarrow{R_0} & x_1 & \dashrightarrow & x_{r-1} & \xrightarrow{R_{r-1}} & E(x_0) \\
\downarrow A_0 & & \downarrow A_1 & \circlearrowleft & \downarrow A_{r-1} & & \downarrow A_r \\
z_0 & \xrightarrow[R_0]{} & z_1 & \dashrightarrow & z_{r-1} & \xrightarrow[R_{r-1}]{} & E(z_0)
\end{array}$$

$\Longrightarrow$ **round-by-round** and **layer-by-layer** studies.

Layer-by-layer probability-1 trail

Simplified setting for this presentation

- Commutation only: $E \circ \mathcal{A} = \mathcal{A} \circ E$ (case $\mathcal{A} = \mathcal{B}$)
- Parallel mappings: $\mathcal{A} := A \,||\, A \,||\, \cdots \,||\, A$, where $A \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$.

Layer-by-layer probability-1 trail

Simplified setting for this presentation

- Commutation only: $E \circ \mathcal{A} = \mathcal{A} \circ E$ (case $\mathcal{A} = \mathcal{B}$)
- Parallel mappings: $\mathcal{A} := A \,||\, A \,||\, \cdots \,||\, A$, where $A \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$.

S-box layer

$\mathcal{A} \circ \mathcal{S} = \mathcal{S} \circ \mathcal{A} \iff A \circ S = S \circ A \implies$ self-affine equivalent S-box.

Effective search for small m (4, 8 bits). [EC:BDBP03] [EC:Dinur18]

Layer-by-layer probability-1 trail

Simplified setting for this presentation

- Commutation only: $E \circ \mathcal{A} = \mathcal{A} \circ E$ (case $\mathcal{A} = \mathcal{B}$)
- Parallel mappings: $\mathcal{A} := A \,||\, A \,||\, \cdots \,||\, A$, where $A \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$.

S-box layer

$\mathcal{A} \circ \mathcal{S} = \mathcal{S} \circ \mathcal{A} \iff A \circ S = S \circ A \implies$ self-affine equivalent S-box.

Effective search for small m (4, 8 bits). [EC:BDBP03] [EC:Dinur18]

Constant addition

$T_c(x) := x + c, \quad A(x) := L_A(x) + c_A.$

Layer-by-layer probability-1 trail

Simplified setting for this presentation

- Commutation only: $E \circ \mathcal{A} = \mathcal{A} \circ E$ (case $\mathcal{A} = \mathcal{B}$)
- Parallel mappings: $\mathcal{A} := A \mid\mid A \mid\mid \cdots \mid\mid A$, where $A \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$.

S-box layer

$\mathcal{A} \circ \mathcal{S} = \mathcal{S} \circ \mathcal{A} \iff A \circ S = S \circ A \implies$ self-affine equivalent S-box.

Effective search for small m (4, 8 bits). [EC:BDBP03] [EC:Dinur18]

Constant addition

$T_c(x) := x + c, \quad A(x) := L_A(x) + c_A.$

$$A \circ T_c(x) = L_A(x) + L_A(c) + c_A \quad \text{and} \quad T_c \circ A(x) = L_A(x) + c + c_A$$

Layer-by-layer probability-1 trail

Simplified setting for this presentation

- Commutation only: $E \circ \mathcal{A} = \mathcal{A} \circ E$ (case $\mathcal{A} = \mathcal{B}$)
- Parallel mappings: $\mathcal{A} := A \,||\, A \,||\, \cdots \,||\, A$, where $A \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$.

S-box layer

$\mathcal{A} \circ \mathcal{S} = \mathcal{S} \circ \mathcal{A} \iff A \circ S = S \circ A \implies$ self-affine equivalent S-box.

Effective search for small m (4, 8 bits). [EC:BDBP03] [EC:Dinur18]

Constant addition

$T_c(x) := x + c, \quad A(x) := L_A(x) + c_A.$

$$A \circ T_c(x) = L_A(x) + L_A(c) + c_A \quad \text{and} \quad T_c \circ A(x) = L_A(x) + c + c_A$$

$A \circ T_c = T_c \circ A \iff c \in \mathrm{Fix}(L_A).$

Layer-by-layer probability-1 trail

Simplified setting for this presentation

- Commutation only: $E \circ \mathcal{A} = \mathcal{A} \circ E$ (case $\mathcal{A} = \mathcal{B}$)
- Parallel mappings: $\mathcal{A} := A \,||\, A \,||\, \cdots \,||\, A$, where $A \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$.

S-box layer

$\mathcal{A} \circ \mathcal{S} = \mathcal{S} \circ \mathcal{A} \iff A \circ S = S \circ A \implies$ self-affine equivalent S-box.

Effective search for small m (4, 8 bits). [EC:BDBP03] [EC:Dinur18]

Constant addition

$T_c(x) := x + c, \quad A(x) := L_A(x) + c_A.$

$$A \circ T_c(x) = L_A(x) + L_A(c) + c_A \quad \text{and} \quad T_c \circ A(x) = L_A(x) + c + c_A$$

$A \circ T_c = T_c \circ A \iff c \in \mathrm{Fix}(L_A).$

Linear layer

Let $\mathcal{L} = (\mathcal{L}_{ij})$ be an invertible block matrix with m-size blocks $\mathcal{L}_{ij}$.

$\mathcal{L} \circ \mathcal{A} = \mathcal{A} \circ \mathcal{L} \iff \mathcal{L}_{ij} \circ L_A = L_A \circ \mathcal{L}_{ij}$ for all i, j and $c_A \in \mathrm{Fix}(\mathcal{L})$.

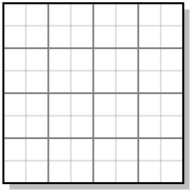
Midori [AC:BBISHA15] in a nutshell

A (not so) standard SPN

- AES-like,
- Standard wide-trail analysis,
- . . . yet weak-key probability-1 (non)-linear approximations [TLS19, Bey18]
- due to (excessive) lightweightness and sparsity.

The round function

$$p = AK \circ AC \circ MC \circ PC \circ S$$

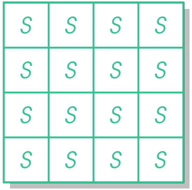


A (not so) standard SPN

- AES-like,
- Standard wide-trail analysis,
- ...yet weak-key probability-1 (non)-linear approximations [TLS19, Bey18]
- due to (excessive) lightweightness and sparsity.

The round function

$$p = AK \circ AC \circ MC \circ PC \circ S$$

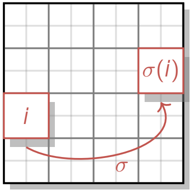


A (not so) standard SPN

- AES-like,
- Standard wide-trail analysis,
- ...yet weak-key probability-1 (non)-linear approximations [TLS19, Bey18]
- due to (excessive) lightweightness and sparsity.

The round function

$$p = AK \circ AC \circ MC \circ PC \circ S$$

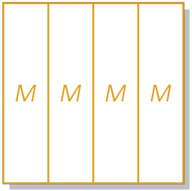


A (not so) standard SPN

- AES-like,
- Standard wide-trail analysis,
- ...yet weak-key probability-1 (non)-linear approximations [TLS19, Bey18]
- due to (excessive) lightweightness and sparsity.

The round function

$$p = AK \circ AC \circ MC \circ PC \circ S$$



$$M = \begin{pmatrix} 0 & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & 0 & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & 0 & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & 0 \end{pmatrix}$$

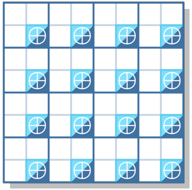
Midori [AC:BBISHA15] in a nutshell

A (not so) standard SPN

- AES-like,
- Standard wide-trail analysis,
- ...yet weak-key probability-1 (non)-linear approximations [TLS19, Bey18]
- due to (excessive) lightweightness and sparsity.

The round function

$$p = AK \circ AC \circ MC \circ PC \circ S$$



Midori [AC:BBISHA15] in a nutshell

A (not so) standard SPN

- AES-like,
- Standard wide-trail analysis,
- ...yet weak-key probability-1 (non)-linear approximations [TLS19, Bey18]
- due to (excessive) lightweightness and sparsity.

The round function

$$p = AK \circ AC \circ MC \circ PC \circ S$$

$K = (K_0||K_1) \in \mathbb{F}_2^{128}$
K_0 for even rounds
K_1 for odd ones.

Midori with weak constants

$$p = AK \circ AC \circ MC \circ PC \circ S$$

Midori with weak constants

$$p = AK \circ AC \circ MC \circ PC \circ S$$

Sbox layer

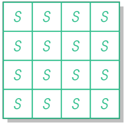
There exists a single non-trivial $A^\star$ st. $A^\star \circ S = S \circ A^\star$.

S	S	S	S
S	S	S	S
S	S	S	S
S	S	S	S

$$p = AK \circ AC \circ MC \circ PC \circ S$$

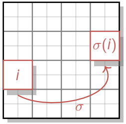
Sbox layer

There exists a single non-trivial $A^\star$ st. $A^\star \circ S = S \circ A^\star$.



Cells permutation

Parallel mapping $\mathcal{A}$: free commutation.

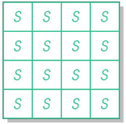


Midori with weak constants

$$p = AK \circ AC \circ MC \circ PC \circ S$$

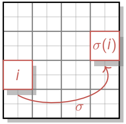
Sbox layer

There exists a single non-trivial $A^\star$ st. $A^\star \circ S = S \circ A^\star$.



Cells permutation

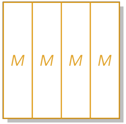
Parallel mapping $\mathcal{A}$: free commutation.



Linear layer

- $M_{ij} \circ L_A = L_A \circ M_{ij}\ \forall\, i, j$. But $M_{ij} \in \{0_4, \mathrm{Id}_4\}$.
- $c_{\mathcal{A}} \in \mathrm{Fix}(\mathcal{L})$. But $M(c, c, c, c) = (c, c, c, c)$ for any c.

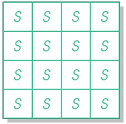
$\implies$ Any $\mathcal{A}$ would work.



$$p = AK \circ AC \circ MC \circ PC \circ S$$

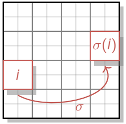
Sbox layer

There exists a single non-trivial $A^\star$ st. $A^\star \circ S = S \circ A^\star$.



Cells permutation

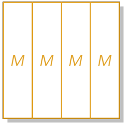
Parallel mapping $\mathcal{A}$: free commutation.



Linear layer

- $M_{ij} \circ L_A = L_A \circ M_{ij}\ \forall\, i, j$. But $M_{ij} \in \{0_4, \mathrm{Id}_4\}$.
- $c_{\mathcal{A}} \in \mathrm{Fix}(\mathcal{L})$. But $M(c, c, c, c) = (c, c, c, c)$ for any c.

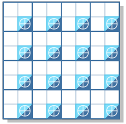
$\Longrightarrow$ Any $\mathcal{A}$ would work.



Constants

$\mathrm{Fix}(L_{A^\star}) = \langle \mathtt{0x2}, \mathtt{0x5}, \mathtt{0x8} \rangle$. $\rightsquigarrow$ Consider **variants** with modified constants.

Weak keys: 1-bit condition per nibble $\rightsquigarrow 2^{96}$ out of 2^{128}.



Midori with weak constants, part 2

Recap

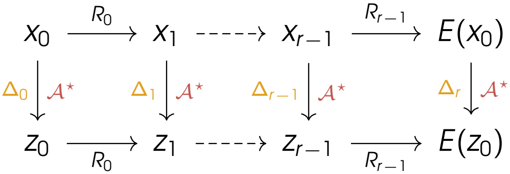
$\mathcal{A}^\star \circ P = P \circ \mathcal{A}^\star$ for every layer P (given weak constants/keys).

$\mathcal{A}^\star \circ E_k = E_k \circ \mathcal{A}^\star$ for $1/2^{32}$ of the keys k.

$$\begin{array}{ccccccc} x_0 & \xrightarrow{R_0} & x_1 & \dashrightarrow & x_{r-1} & \xrightarrow{R_{r-1}} & E(x_0) \\ \downarrow \mathcal{A}^\star & & \downarrow \mathcal{A}^\star & & \downarrow \mathcal{A}^\star & & \downarrow \mathcal{A}^\star \\ z_0 & \xrightarrow[R_0]{} & z_1 & \dashrightarrow & z_{r-1} & \xrightarrow[R_{r-1}]{} & E(z_0) \end{array}$$

$$\mathbb{P}_{x \xleftarrow{\$} X}(\underbrace{\mathcal{A}^\star \to \mathcal{A}^\star \to \cdots \to \mathcal{A}^\star}_{r \text{ times}}) = 1, \quad \text{for any } r!$$

Midori with weak constants, part 3



$$\Delta_i := x_i \oplus z_i = x_i \oplus \mathcal{A}^\star(x_i)$$

Midori with weak constants, part 3

$$
\begin{array}{ccccccc}
x_0 & \xrightarrow{R_0} & x_1 & \dashrightarrow & x_{r-1} & \xrightarrow{R_{r-1}} & E(x_0) \\
\Delta_0 \downarrow \mathcal{A}^\star & & \Delta_1 \downarrow \mathcal{A}^\star & & \Delta_{r-1} \downarrow \mathcal{A}^\star & & \Delta_r \downarrow \mathcal{A}^\star \\
z_0 & \xrightarrow[R_0]{} & z_1 & \dashrightarrow & z_{r-1} & \xrightarrow[R_{r-1}]{} & E(z_0)
\end{array}
$$

$$\Delta_i := x_i \oplus z_i = x_i \oplus \mathcal{A}^\star(x_i)$$

Surprising differential interpretation

$\delta = \texttt{0xf}, \quad \delta' = \texttt{0xa}.$

$\forall\ \Delta \in \{\delta, \delta'\}^{16},\ \mathbb{P}_{x \xleftarrow{\$} X}(x + \mathcal{A}^\star(x) = \Delta) = 2^{-16} \iff (x, x + \Delta) = (x, \mathcal{A}^\star(x))$ with proba 2^{-16}

Midori with weak constants, part 3

$$\begin{array}{ccccccc}
x_0 & \xrightarrow{R_0} & x_1 & \dashrightarrow & x_{r-1} & \xrightarrow{R_{r-1}} & E(x_0) \\
\Delta_0 \big\downarrow \mathcal{A}^\star & & \Delta_1 \big\downarrow \mathcal{A}^\star & & \Delta_{r-1} \big\downarrow \mathcal{A}^\star & & \Delta_r \big\downarrow \mathcal{A}^\star \\
z_0 & \xrightarrow[R_0]{} & z_1 & \dashrightarrow & z_{r-1} & \xrightarrow[R_{r-1}]{} & E(z_0)
\end{array}$$

$$\Delta_i := x_i \oplus z_i = x_i \oplus \mathcal{A}^\star(x_i)$$

Surprising differential interpretation

$\delta = \texttt{0xf}, \quad \delta' = \texttt{0xa}.$

$$\forall\ \Delta \in \{\delta, \delta'\}^{16},\ \mathbb{P}_{x \xleftarrow{\$} X}(x + \mathcal{A}^\star(x) = \Delta) = 2^{-16} \iff (x, x + \Delta) = (x, \mathcal{A}^\star(x)) \text{ with proba } 2^{-16}$$

$$\Delta \xrightarrow{2^{-16}} \mathcal{A}^\star \xrightarrow{1} \cdots \xrightarrow{1} \mathcal{A}^\star \xrightarrow{2^{-16}} \Delta$$

Weak-key Differential interpretation

Recap

If k is **weak**:

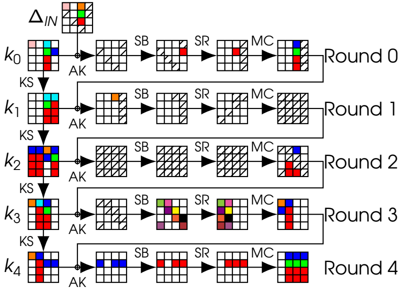
- $\mathbb{P}_{x \xleftarrow{\$} X}(\Delta \to \Delta') = 2^{-32}$ for any $\Delta, \Delta' \in \{\delta, \delta'\}^{16}$.
- $\mathbb{P}_{x \xleftarrow{\$} X}\left(\Delta \to \{\delta, \delta'\}^{16}\right) = 2^{-16}$ for any $\Delta \in \{\delta, \delta'\}^{16}$.
- For any number of rounds, activate all S-boxes.

Recap

If k is **weak**:

- $\mathbb{P}_{x \xleftarrow{\$} X}(\Delta \to \Delta') = 2^{-32}$ for any $\Delta, \Delta' \in \{\delta, \delta'\}^{16}$.
- $\mathbb{P}_{x \xleftarrow{\$} X}(\Delta \to \{\delta, \delta'\}^{16}) = 2^{-16}$ for any $\Delta \in \{\delta, \delta'\}^{16}$.
- For any number of rounds, activate all S-boxes.

Standard case : quite low $\mathbb{P}_{k,x}$



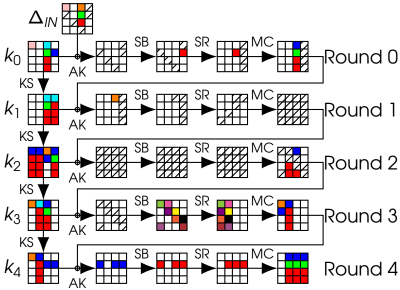
Part of 9-round chosen-key distinguisher for AES-128.
Figure by J. Jean, extracted from Tikz for Cryptographers [Jean16].

Recap

If k is **weak**:

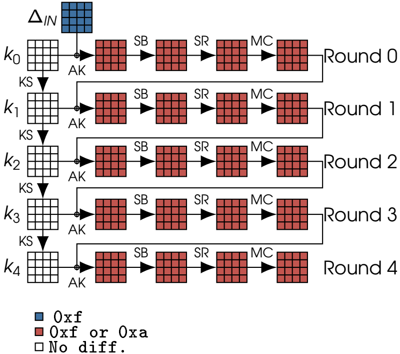
- $\mathbb{P}_{x \xleftarrow{\$} X}(\Delta \to \Delta') = 2^{-32}$ for any $\Delta, \Delta' \in \{\delta, \delta'\}^{16}$.
- $\mathbb{P}_{x \xleftarrow{\$} X}(\Delta \to \{\delta, \delta'\}^{16}) = 2^{-16}$ for any $\Delta \in \{\delta, \delta'\}^{16}$.
- For any number of rounds, activate all S-boxes.

Standard case : quite low $\mathbb{P}_{k,x}$

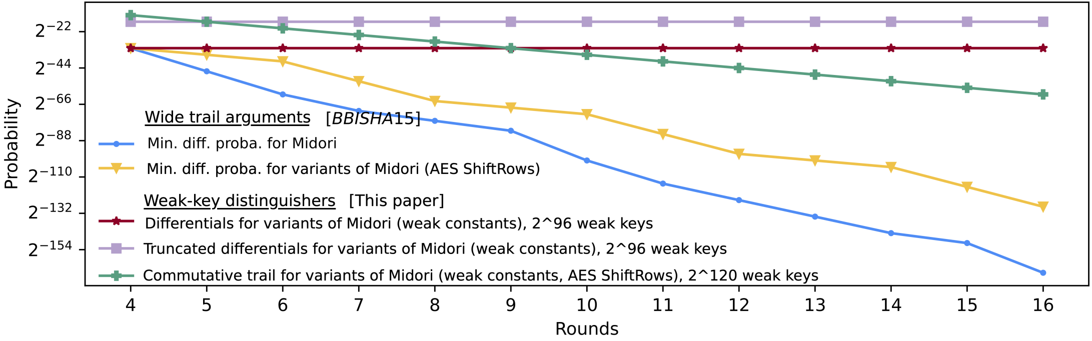


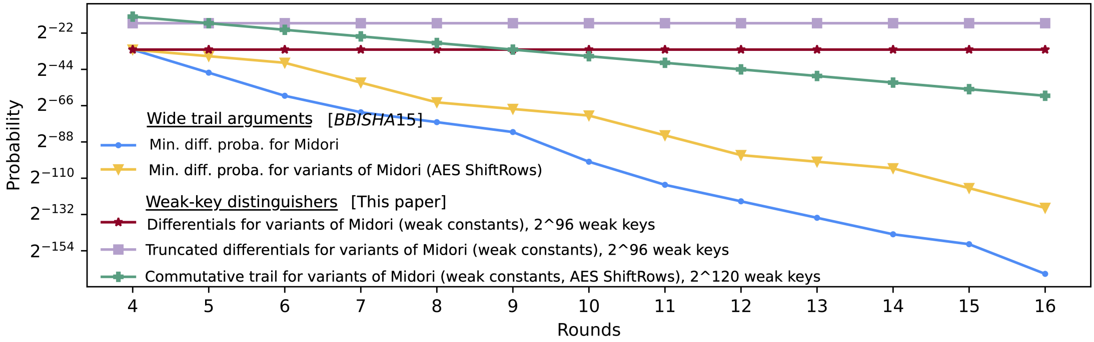
Part of 9-round chosen-key distinguisher for AES-128.
Figure by J. Jean, extracted from Tikz for Cryptographers [Jean16].

This work: high $\mathbb{P}_x$ for some k



Weak-key Differential interpretation, part 2





Caution

- Same observations for the CAESAR candidate SCREAM (see paper).
- Same idea can be used to hide probability-1 differential trails [C:BFLNS23].

Good news

Probability-1 commutative trails can be automatically detected !

A bigger weak-key space ?

WK space

Fewer "active" S-boxes $\Longrightarrow$ bigger weak-key space.

$$\begin{pmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{pmatrix} \rightsquigarrow \begin{pmatrix} A & \mathrm{Id} & A & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ A & \mathrm{Id} & A & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \end{pmatrix}$$

A bigger weak-key space ?

WK space

Fewer "active" S-boxes $\Longrightarrow$ bigger weak-key space.

$$\begin{pmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{pmatrix} \rightsquigarrow \begin{pmatrix} A & \mathrm{Id} & A & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ A & \mathrm{Id} & A & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \end{pmatrix}$$

Modified-Midori study

- Constants : 4 active nibbles = 4-bit conditions.
- S-box: $S \circ A^\star = A^\star \circ S \quad S \circ \mathrm{Id} = \mathrm{Id} \circ S$
- Cell permutation: Invariant pattern for AES ShiftRows
- $\mathbb{P}_{x \xleftarrow{\$} X} (\mathcal{A}^\star \circ \mathcal{M}(x) = \mathcal{M} \circ \mathcal{A}^\star(x)) = 2^{-4}$.

A bigger weak-key space ?

WK space

Fewer "active" S-boxes $\Longrightarrow$ bigger weak-key space.

$$\begin{pmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{pmatrix} \leadsto \begin{pmatrix} A & \mathrm{Id} & A & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ A & \mathrm{Id} & A & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \end{pmatrix}$$

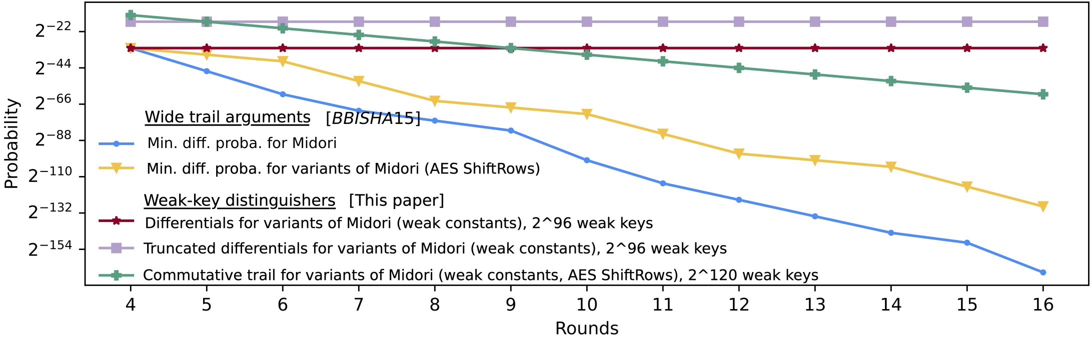
Modified-Midori study

- Constants : 4 active nibbles = 4-bit conditions.
- S-box: $S \circ A^{\star} = A^{\star} \circ S \quad S \circ \mathrm{Id} = \mathrm{Id} \circ S$
- Cell permutation: Invariant pattern for AES ShiftRows
- $\mathbb{P}_{x \xleftarrow{\$} X} (\mathcal{A}^{\star} \circ \mathcal{M}(x) = \mathcal{M} \circ \mathcal{A}^{\star}(x)) = 2^{-4}$.

WK-space / probability trade-off

For 2^{120} weak keys, $\mathbb{P}_{x \xleftarrow{\$} X} (R \circ \mathcal{M}(x) = \mathcal{M} \circ R(x)) = 2^{-4}$.

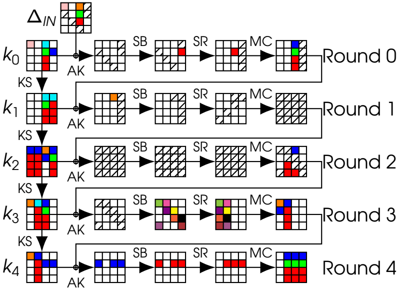
A bigger weak-key space ? part 2



What was done

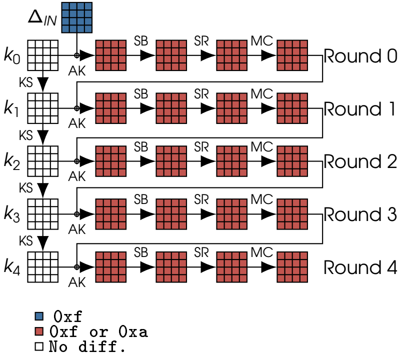
- Probability-1: automatically solved (paper + github)
- Probabilistic commutative trails: way-harder to study but weak-key study

Standard case : quite low $\mathbb{P}_{k,x}$



Part of 9-round chosen-key distinguisher for AES-128.
Figure by J. Jean, extracted from Tikz for Cryptographers [Jean16].

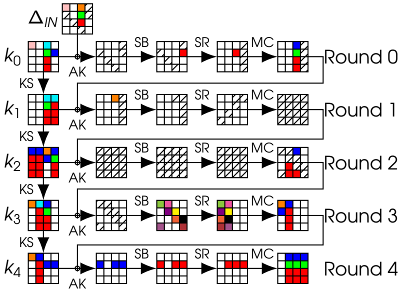
This work: high $\mathbb{P}_x$ for some weak k



What was done

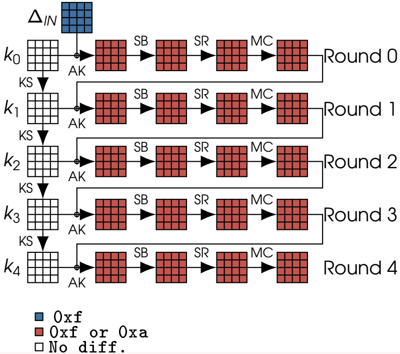
- Probability-1: automatically solved (paper + github)
- Probabilistic commutative trails: way-harder to study but weak-key study

Standard case : quite low $\mathbb{P}_{k,x}$



Part of 9-round chosen-key distinguisher for AES-128.
Figure by J. Jean, extracted from Tikz for Cryptographers [Jean16].

This work: high $\mathbb{P}_x$ for some weak k



Further studies

- Algorithm for probabilistic affine-equivalence.
- Relationships with [C:BeyRij22] ? with invariant subspace cryptanalysis ?
- Hybridization: *e.g.* commutative-differential ?

Recap

For Modified-Midori with ShiftRows and weak-key, $\mathbb{P}_{x \xleftarrow{\$} X} (R \circ \mathcal{A}(x) = \mathcal{A} \circ R(x)) = 2^{-4}$.