On nonlinear approximations and the linear hull effect

Anne Canteaut, Christof Beierle, Gregor Leander

On nonlinear approximations and the linear hull effect

Anne Canteaut
Inria, Paris, France

joint work with Christof Beierle and Gregor Leander

ASK 2018, Kolkota

Linear approximations

Linear approximations

$$\Pr[\alpha \cdot x + \beta \cdot F(x) = 0] \text{ far from } \frac{1}{2}$$

quantified by:

$$\mathrm{cor}_F(\alpha, \beta) = 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha \cdot x + \beta \cdot F(x)}$$

since

$$\Pr[\alpha \cdot x + \beta \cdot F(x) = 0] = \frac{1}{2}(1 + \mathrm{cor}_F(\alpha, \beta))$$

Linear approximations with correlation ± 1

F has a linear approximation with correlation ± 1
iff it has a component of degree 1.

$\Rightarrow$ This never occurs for one-round SPN (except for trivial Sboxes)

An alternative formulation:

$$\mathrm{cor}_F(\alpha, \beta) = -1 + 2^{-n+2} \#\{x \in \langle \alpha \rangle^{\perp} \text{ such that } F(x) \in \langle \beta \rangle^{\perp}\}$$

$$\Rightarrow \mathrm{cor}_F(\alpha, \beta) = \pm 1 \text{ iff } F(\langle \alpha \rangle^{\perp}) = \langle \beta \rangle^{\perp} \text{ or } \mathbb{F}_2^n \setminus \langle \beta \rangle^{\perp}.$$

Linear approximations over several rounds [Daemen 95][Nyberg 01]

$$\mathrm{cor}_{G\circ F}(\alpha, \beta) = \sum_{\gamma \in \mathbb{F}_2^n} \mathrm{cor}_F(\alpha, \gamma)\, \mathrm{cor}_G(\gamma, \beta)\ .$$

If one dominant trail $(\alpha, \gamma_0, \beta)$:

$$\mathrm{cor}_{G\circ F}(\alpha, \beta) \simeq \mathrm{cor}_F(\alpha, \gamma_0)\, \mathrm{cor}_G(\gamma_0, \beta)\ .$$

Otherwise, linear hull effect.

Two-round approximations with correlation ± 1

For a two-round SPN

$$\mathbf{cor}_{L \circ S}(\alpha, \beta) = \sum_{\gamma \in \mathbb{F}_2^n} \mathbf{cor}_S(\alpha, \gamma)\, \mathbf{cor}_L(\gamma, \beta) = \mathbf{cor}_S(\alpha, L^T(\beta))\ .$$

$$\mathbf{cor}_{\mathcal{R} \circ \mathsf{Add}_k \circ \mathcal{R}}(\alpha, \beta) = \sum_{\gamma \in \mathbb{F}_2^n} (-1)^{k \cdot \gamma}\, \mathbf{cor}_S(\alpha, L^T(\gamma))\, \mathbf{cor}_S(\gamma, L^T(\beta))\ .$$

Question: can we get a correlation $\pm\mathbf{1}$ for a two-round approximation for some fixed k?

Nonlinear approximations and invariants

Nonlinear approximations

Let g and h be two balanced Boolean functions of n variables.

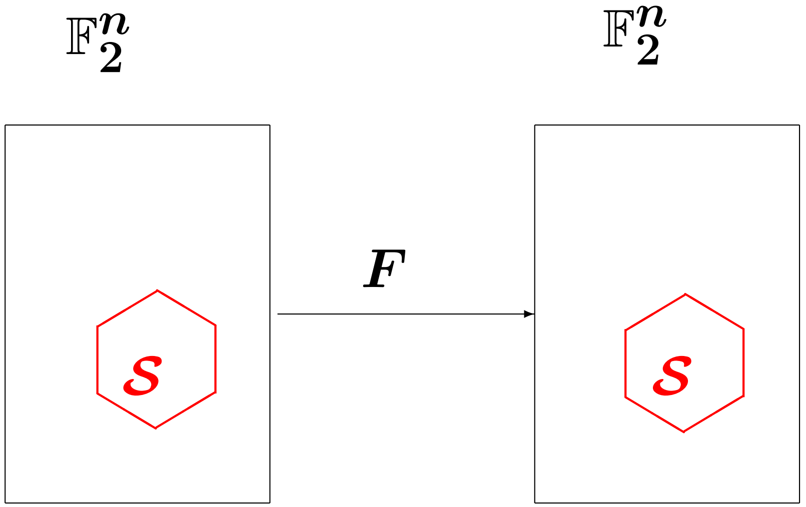
$$\Pr[g(x) + h(F(x)) = 0] \text{ far from } \frac{1}{2}.$$

quantified by:

$$\mathrm{cor}_F(g, h) = 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x)+h(F(x))}$$

Nonlinear invariants [Todo-Leander-Sasaki 16]

Non-trivial partition of $\mathbb{F}_2^n$ invariant under F:



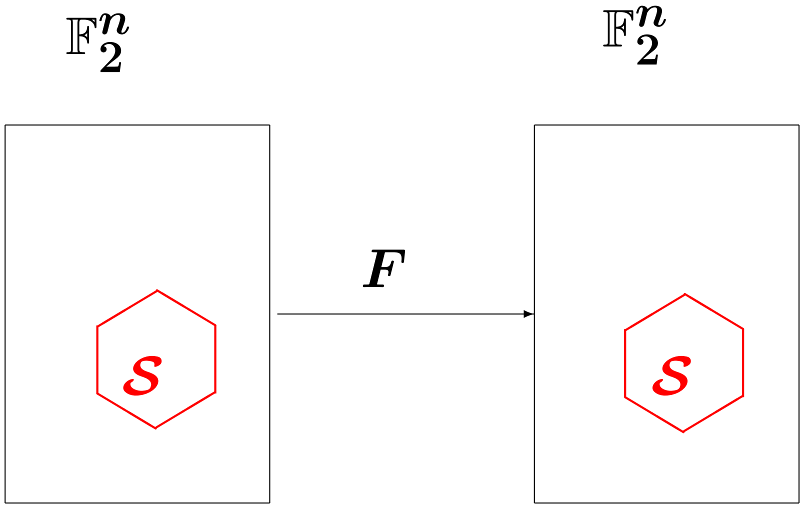
$\mathcal{S}$: any subset of $\mathbb{F}_2^n$

$$F(\mathcal{S}) = \mathcal{S}$$

or $F(\mathcal{S}) = \mathbb{F}_2^n \setminus \mathcal{S}$

The nonlinear invariant attack [Todo-Leander-Sasaki 16]

Non-trivial partition of $\mathbb{F}_2^n$ invariant under F:



$\mathcal{S}$: any subset of $\mathbb{F}_2^n$

$F(\mathcal{S}) = \mathcal{S}$

or $F(\mathcal{S}) = \mathbb{F}_2^n \setminus \mathcal{S}$

Equivalently:

Let g be the Boolean function defined by $g(x) := 1$ iff $x \in \mathcal{S}$

$$\forall x \in \mathbb{F}_2^n, g(F(x)) = g(x) \text{ or } \forall x \in \mathbb{F}_2^n, g(F(x)) = g(x) + 1$$

Such a g is called an invariant for F.

Nonlinear approximations with correlation ± 1

g is an invariant for F if and only if

$$\mathrm{cor}_F(g, g) = 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x)+g(F(x))} = \pm 1$$

Nonlinear approximations as a combination of linear approximations

$$\mathbf{cor}_{\boldsymbol{F}}(\boldsymbol{g},\boldsymbol{h}) = \sum_{\boldsymbol{\gamma},\boldsymbol{\gamma}' \in \mathbb{F}_2^n} \mathbf{cor}_{\boldsymbol{g}}(\boldsymbol{\gamma})\,\mathbf{cor}_{\boldsymbol{F}}(\boldsymbol{\gamma},\boldsymbol{\gamma}')\,\mathbf{cor}_{\boldsymbol{h}}(\boldsymbol{\gamma}') \;.$$

If $\boldsymbol{g} = \boldsymbol{\ell}_{\boldsymbol{\alpha}}$ and $\boldsymbol{h} = \boldsymbol{\ell}_{\boldsymbol{\beta}}$, then

$$\mathbf{cor}_{\boldsymbol{F}}(\boldsymbol{g},\boldsymbol{h}) = \mathbf{cor}_{\boldsymbol{F}}(\boldsymbol{\alpha},\boldsymbol{\beta}) \;.$$

Otherwise, we gather together several linear approximations.

Nonlinear approximations

and the linear hull effect

Transforming nonlinear invariants into linear approximations

Let $\boldsymbol{g}$ be a balanced nonlinear invariant for $\boldsymbol{F}$.

We can always define a permutation $\mathcal{G}$ such that $\boldsymbol{\alpha} \cdot \mathcal{G}(\boldsymbol{x}) = \boldsymbol{g}(\boldsymbol{x})$.

Then,

$$\begin{aligned} \boldsymbol{g}(\boldsymbol{x}) + \boldsymbol{g}(\boldsymbol{F}(\boldsymbol{x})) &= \boldsymbol{\alpha} \cdot \mathcal{G}(\boldsymbol{x}) + \boldsymbol{\alpha} \cdot (\mathcal{G} \circ \boldsymbol{F})(\boldsymbol{x}) \\ &= \boldsymbol{\alpha} \cdot \boldsymbol{y} + \boldsymbol{\alpha} \cdot (\mathcal{G} \circ \boldsymbol{F} \circ \mathcal{G}^{-1})(\boldsymbol{y}) \end{aligned}$$

The nonlinear approximation of $\boldsymbol{F}$ defined by $(\boldsymbol{g}, \boldsymbol{g})$ corresponds to the linear approximation $(\boldsymbol{\alpha}, \boldsymbol{\alpha})$ of $\boldsymbol{F}^{\mathcal{G}, \mathcal{G}^{-1}} = \mathcal{G} \circ \boldsymbol{F} \circ \mathcal{G}^{-1}$.

$$\mathbf{cor}_{\boldsymbol{F}^{\mathcal{G}, \mathcal{G}^{-1}}}(\boldsymbol{\alpha}, \boldsymbol{\alpha}) = \sum_{\gamma_1, \gamma_2 \in \mathbb{F}_2^n} \mathbf{cor}_{\mathcal{G}_\alpha}(\gamma_1)\, \mathbf{cor}_{\boldsymbol{F}}(\gamma_1, \gamma_2)\, \mathbf{cor}_{\mathcal{G}_\alpha}(\gamma_2)$$

The other components of $\mathcal{G}$ do not matter!

$\mathcal{G}$-shifted trails

$$
\begin{aligned}
E^{\mathcal{G},\mathcal{G}^{-1}}_{(k_0,\ldots,k_t)} &= \mathcal{G} \circ \mathcal{R}_{k_t} \circ \mathcal{R}_{k_{t-1}} \circ \cdots \circ \mathcal{R}_{k_0} \circ \mathcal{G}^{-1} \\
&= \mathcal{R}^{\mathcal{G},\mathcal{G}^{-1}}_{k_t} \circ \mathcal{R}^{\mathcal{G},\mathcal{G}^{-1}}_{k_{t-1}} \circ \cdots \circ \mathcal{R}^{\mathcal{G},\mathcal{G}^{-1}}_{k_0} .
\end{aligned}
$$

$$
\mathrm{cor}_{E^{\mathcal{G},\mathcal{G}^{-1}}_{(k_0,\ldots,k_t)}}(\alpha, \beta) = \sum_{\gamma_1,\ldots,\gamma_{t-1} \in \mathbb{F}_2^n} \prod_{i=0}^{t-1} \mathrm{cor}_{\mathcal{R}^{\mathcal{G},\mathcal{G}^{-1}}_{k_i}}(\gamma_i, \gamma_{i+1}) \, .
$$

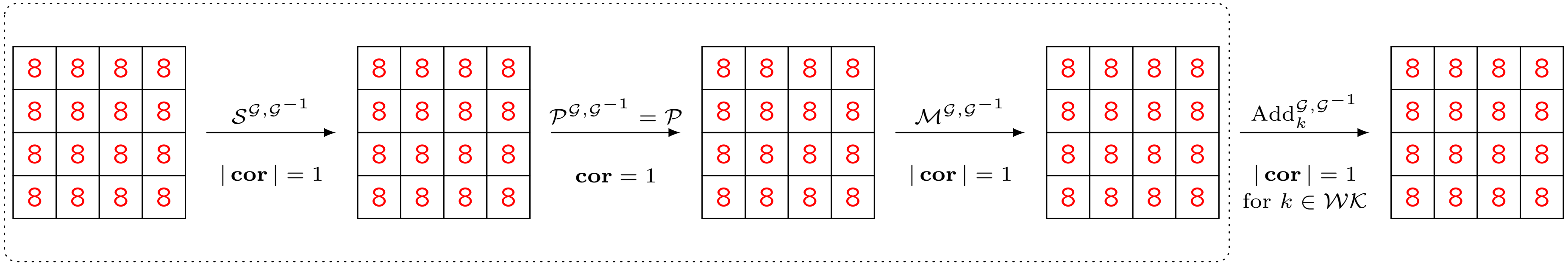
A one-round $\mathcal{G}$-shifted trail on Midori-64

$\mathcal{G} = (G, \ldots, G)$ where G is a bijection on 4 bits such that $\langle 8, G(x) \rangle = g(x)$ with $g(x) = x_3x_2 + x_2 + x_1 + x_0$ invariant for the Sbox, i.e.

$$|\,\mathbf{cor}_{S^{G,G^{-1}}}(8,8)| = 1\ .$$

$$|\,\mathbf{cor}_{\mathcal{M}^{\mathcal{G},\mathcal{G}^{-1}}}((8,\ldots,8),(8,\ldots,8))\,| = 1\ .$$

$\Rightarrow$ Iterative one-round trail with correlation ± 1:



A two-round shifted trail on Midori-64 [Beyne 18]

For $g(x) = x_0x_2 + x_0 + x_1 + x_3$ and $\alpha =$ 0x5, the Sbox satisfies

$$g(S(x)) + \alpha \cdot x = 1 \; .$$

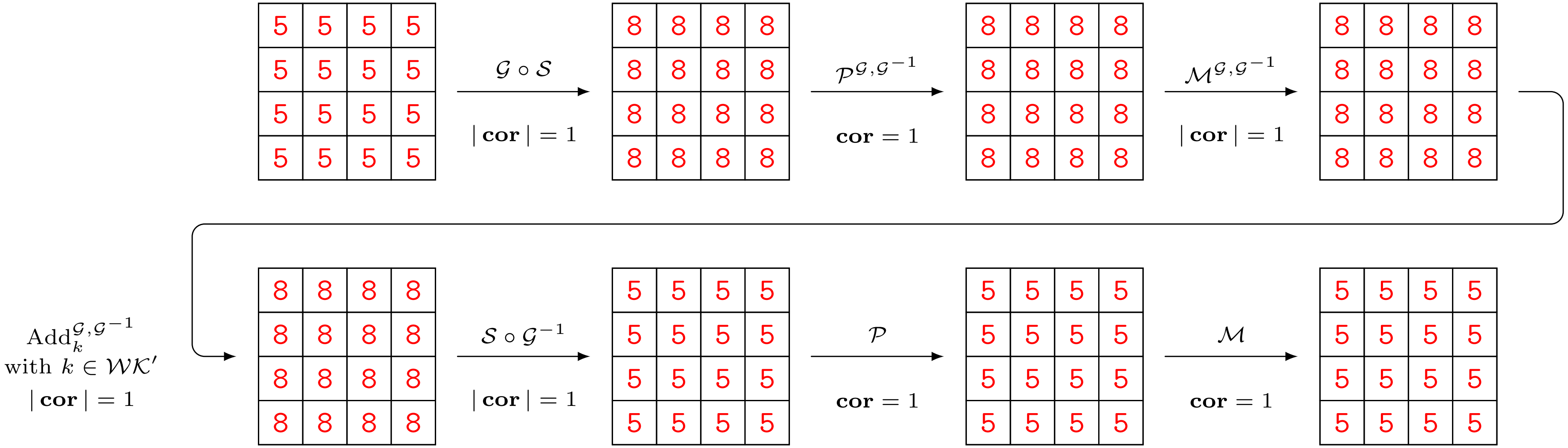
We choose a 4-bit bijection G such that $\langle 8, G(x)\rangle = g(x)$.

Equivalently,

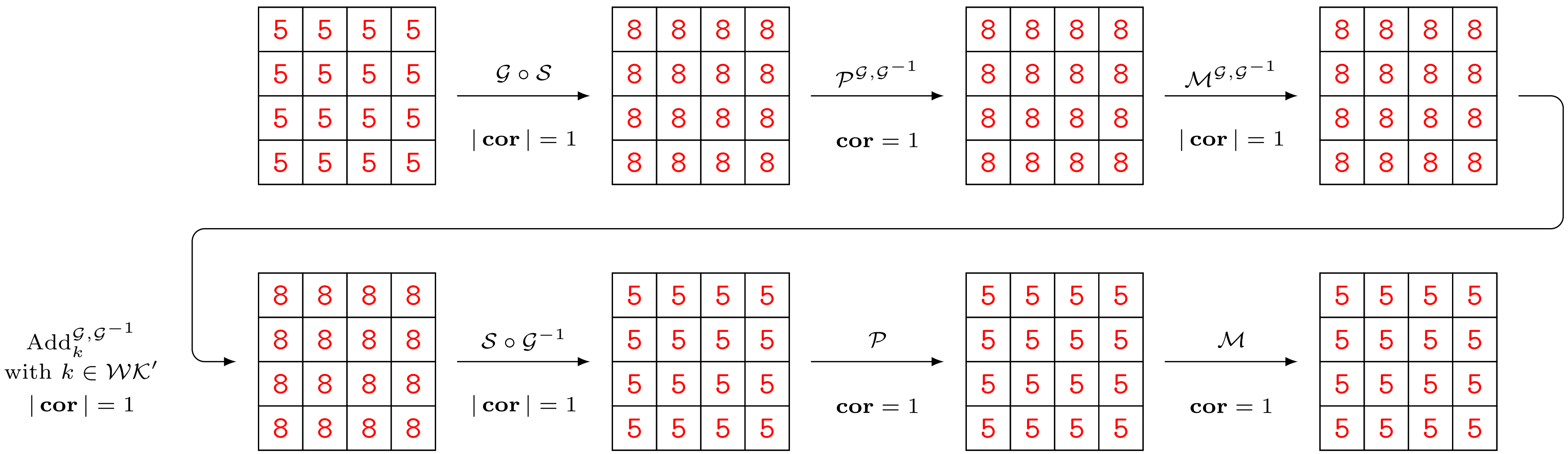
$$\mathrm{cor}_S(\ell_\alpha, g) = \mathrm{cor}_{G \circ S}(\alpha, 8) = -1 \; .$$

$$|\, \mathrm{cor}_{\mathcal{M}^{\mathcal{G},\mathcal{G}^{-1}}}((8, \ldots, 8), (8, \ldots, 8))\,| = 1 \; .$$

A two-round shifted trail on Midori-64 [Beyne 18]



A two-round shifted trail on Midori-64 [Beyne 18]



This is a two-round linear approximation with correlation $\pm\mathbf{1}$!

A 4-round $\mathcal{G}$-shifted trail on Midori-64

G is a bijection on 4 bits such that $\langle 8, G(x)\rangle = g(x)$
with $g(x) = x_3x_2x_1 + x_3x_1 + x_3 + x_2 + x_1 + x_0$ invariant for the Sbox:

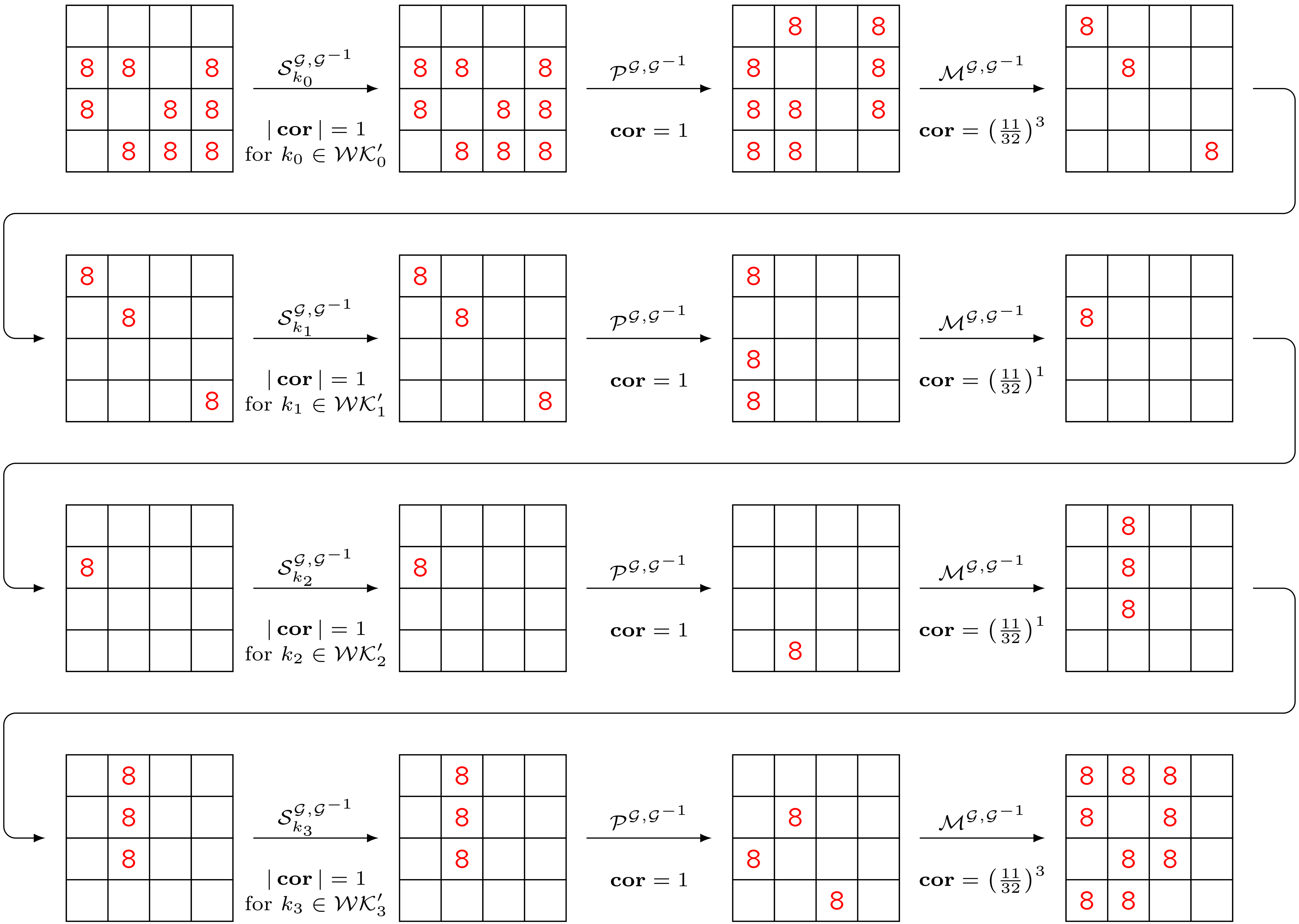
$$|\,\mathbf{cor}_{S^{G,G^{-1}}}(8,8)| = 1\ .$$

But,

$$|\,\mathbf{cor}_{\mathrm{M}^{\mathrm{G},\mathrm{G}^{-1}}}(\alpha, \mathrm{M}\alpha)\,| = \frac{11}{32}$$

if $\alpha \neq (0,0,0,0)$ and all $\alpha_i \in \{0, 8\}$.

A 4-round $\mathcal{G}$-shifted trail on Midori-64



A 4-round $\mathcal{G}$-shifted trail on Midori-64

The weak keys are those equal to $\mathbf{0}$ or $\mathbf{1}$ in all active cells.

Correlation of the trail:

$$\left(\frac{\mathbf{11}}{\mathbf{32}}\right)^{\mathbf{8}} = \mathbf{2^{-12.325}}$$

Correlation of the approximation:

$$\mathbf{cor}_{(\mathcal{R}_{k_3} \circ \ldots \mathcal{R}_{k_0})^{\mathcal{G},\mathcal{G}^{-1}}(\alpha,\alpha)} \simeq \mathbf{2^{-12.16}}$$

What's about the other trails? For the first 2 rounds:

- For $G_1 = [\mathtt{0}, \mathtt{8}, \mathtt{c}, \mathtt{4}, \mathtt{a}, \mathtt{2}, \mathtt{6}, \mathtt{e}, \mathtt{9}, \mathtt{1}, \mathtt{d}, \mathtt{5}, \mathtt{3}, \mathtt{b}, \mathtt{f}, \mathtt{7}]$,
  35,937 $\mathcal{G}_1$-shifted linear trails having a nonzero correlation
- For $G_2 = [\mathtt{0}, \mathtt{9}, \mathtt{a}, \mathtt{1}, \mathtt{8}, \mathtt{2}, \mathtt{3}, \mathtt{f}, \mathtt{c}, \mathtt{4}, \mathtt{d}, \mathtt{5}, \mathtt{6}, \mathtt{e}, \mathtt{b}, \mathtt{7}]$,
  282,184 $\mathcal{G}_2$-shifted linear trails having a nonzero correlation

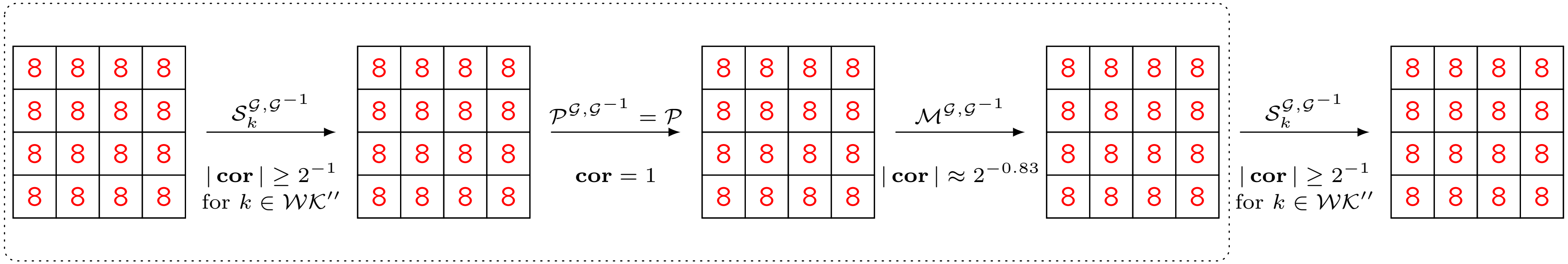
Another 1-round $\mathcal{G}$-shifted trail on Midori-64

$\mathcal{G} = (G', G, \ldots, G)$ where G is a bijection on 4 bits such that $\langle 8, G(x)\rangle = g(x)$ with $g(x) = x_3x_2 + x_2 + x_1 + x_0$ invariant for S, $\langle 8, G'(x)\rangle = g'(x)$ with $g'(x) = x_3x_2x_1 + x_3x_1 + x_3 + x_2 + x_1 + x_0$.

$$|\,\mathrm{cor}_{S_k^{G', G'^{-1}}}(8, 8)| = \begin{cases} 1 & \text{if } k \in \{0,1\} \\ 2^{-1} & \text{if } k \notin \{0,1\} \end{cases} \quad .$$

$$|\,\mathrm{cor}_{\mathcal{M}^{\mathcal{G},\mathcal{G}^{-1}}}((8, \ldots, 8), (8, \ldots, 8))\,| \simeq 2^{-0.83}$$

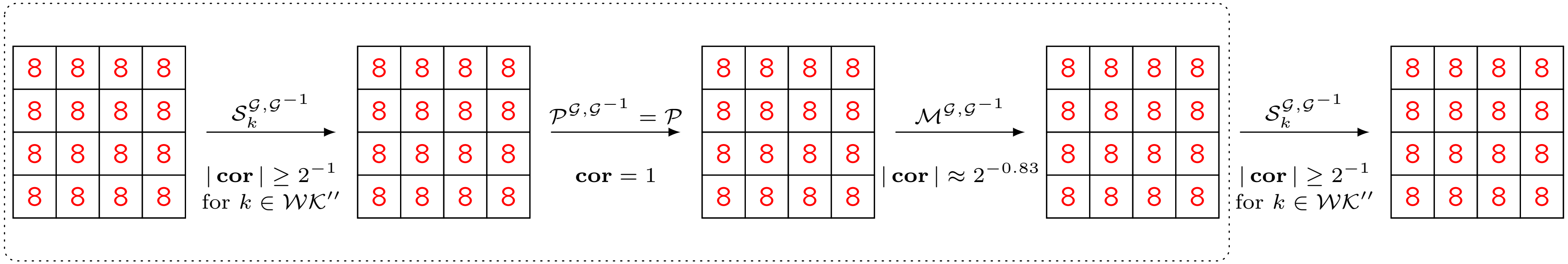
Another 1-round $\mathcal{G}$-shifted trail on Midori-64



Correlation of the 16-round trail:

$$\geq \left(\mathbf{2}^{-\mathbf{1.83}}\right)^{\mathbf{16}} = \mathbf{2}^{-\mathbf{29.28}}$$

Another 1-round $\mathcal{G}$-shifted trail on Midori-64



Correlation of the 16-round trail:

$$\geq \left(\mathbf{2}^{-\mathbf{1.83}}\right)^{\mathbf{16}} = \mathbf{2}^{-\mathbf{29.28}}$$

Correlation over 16 rounds:

different from the correlation of the trail.

Focus on a single column

$\mathcal{G} = (G', G, G, G)$ with

$$|\,\mathbf{cor}_{S_k^{G',G'^{-1}}}(8,8)| = \begin{cases} 1 & \text{if } k \in \{0,1\} \\ 2^{-1} & \text{if } k \notin \{0,1\} \end{cases} .$$

$$|\,\mathbf{cor}_{\mathbf{M}^{\mathcal{G},\mathcal{G}^{-1}}}((8,8,8,8),(8,8,8,8))\,| = 2^{-0.83}$$

$$\begin{bmatrix}8\\8\\8\\8\end{bmatrix} \xrightarrow[|\,\mathbf{cor}\,| \geq 2^{-1}]{\mathcal{S}_{k_0}^{\mathcal{G},\mathcal{G}^{-1}}} \begin{bmatrix}8\\8\\8\\8\end{bmatrix} \xrightarrow[|\,\mathbf{cor}\,| \approx 2^{-0.83}]{\mathbf{M}^{\mathcal{G},\mathcal{G}^{-1}}} \begin{bmatrix}8\\8\\8\\8\end{bmatrix} \xrightarrow[|\,\mathbf{cor}\,| \geq 2^{-1}]{\mathcal{S}_{k_1}^{\mathcal{G},\mathcal{G}^{-1}}} \begin{bmatrix}8\\8\\8\\8\end{bmatrix} \xrightarrow[|\,\mathbf{cor}\,| \approx 2^{-0.83}]{\mathbf{M}^{\mathcal{G},\mathcal{G}^{-1}}} \begin{bmatrix}8\\8\\8\\8\end{bmatrix}$$

If $k_1 \in \left(\mathbb{F}_2^4 \setminus \{(0,0,*,*)\}\right) \times \{(0,0,*,*)\}^3$,

$$\mathbf{cor}_{\mathcal{R}_{k_1} \circ \mathcal{R}_{k_0}}((8,8,8,8),(8,8,8,8)) = 0$$

Open problems

- When can we approximate the correlation with a single trail?
- Nonlinear approximations as a method for clustering linear approximations to capture the linear hull effect?
  - How general is this?
  - How can we find the appropriate approximation?