

On nonlinear approximations and the linear hull effect

Anne Canteaut, Christof Beierle, Gregor Leander

► **To cite this version:**

Anne Canteaut, Christof Beierle, Gregor Leander. On nonlinear approximations and the linear hull effect. ASK 2018 - 8th Asian Workshop on Symmetric Key Cryptography, Nov 2018, Kolkata, India. hal-01955286

HAL Id: hal-01955286

<https://hal.inria.fr/hal-01955286>

Submitted on 14 Dec 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On nonlinear approximations and the linear hull effect

Anne Canteaut
Inria, Paris, France

joint work with Christof Beierle and Gregor Leander

ASK 2018, Kolkata

Linear approximations

Linear approximations

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

quantified by:

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

since

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

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:

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

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

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

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

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

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

Otherwise, linear hull effect.

Two-round approximations with correlation ± 1

For a two-round SPN

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

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

Question: can we get a correlation ± 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.

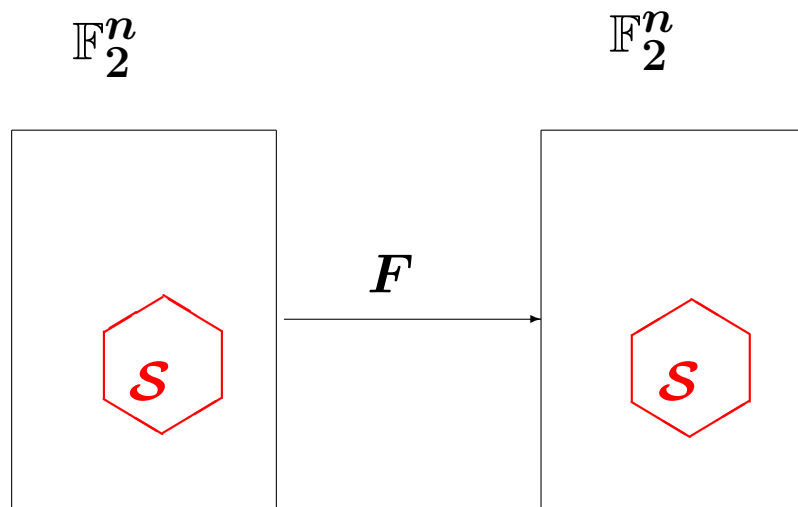
$$\Pr[g(x) + h(F(x)) = 0] \text{ far from } \frac{1}{2}.$$

quantified by:

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

Nonlinear invariants [Todo-Leander-Sasaki 16]

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



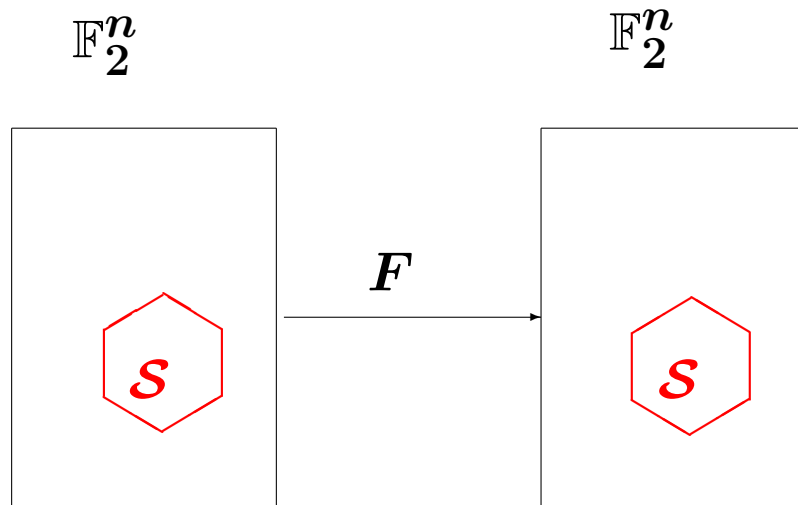
S : any subset of \mathbb{F}_2^n

$$F(S) = S$$

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

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

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

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

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

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

Nonlinear approximations as a combination of linear approximations

$$\text{cor}_F(g, h) = \sum_{\gamma, \gamma' \in \mathbb{F}_2^n} \text{cor}_g(\gamma) \text{cor}_F(\gamma, \gamma') \text{cor}_h(\gamma') .$$

If $g = \ell_\alpha$ and $h = \ell_\beta$, then

$$\text{cor}_F(g, h) = \text{cor}_F(\alpha, \beta) .$$

Otherwise, we gather together several linear approximations.

Nonlinear approximations and the linear hull effect

Transforming nonlinear invariants into linear approximations

Let g be a **balanced** nonlinear invariant for F .

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

Then,

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

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

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

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

\mathcal{G} -shifted trails

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

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

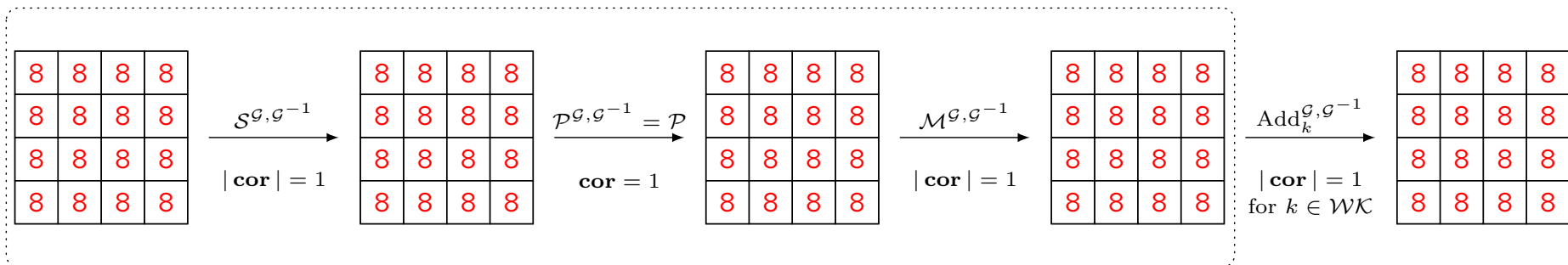
A one-round \mathcal{G} -shifted trail on Midori-64

$\mathcal{G} = (G, \dots, G)$ 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.

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

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

\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

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

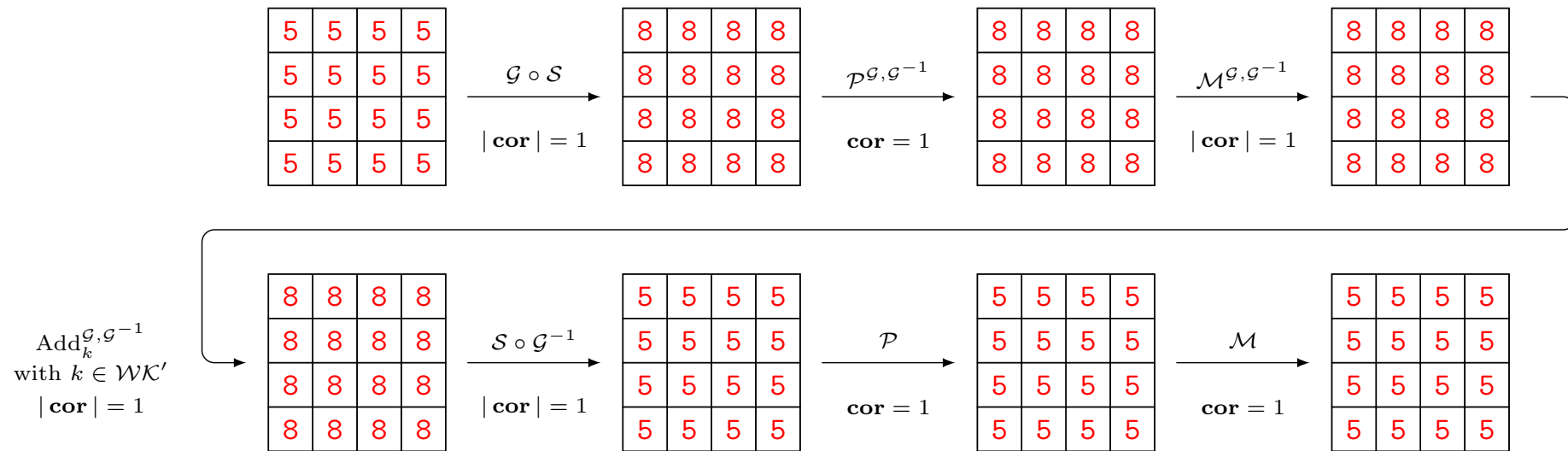
We choose a 4-bit bijection G such that $\langle 8, G(x) \rangle = g(x)$.

Equivalently,

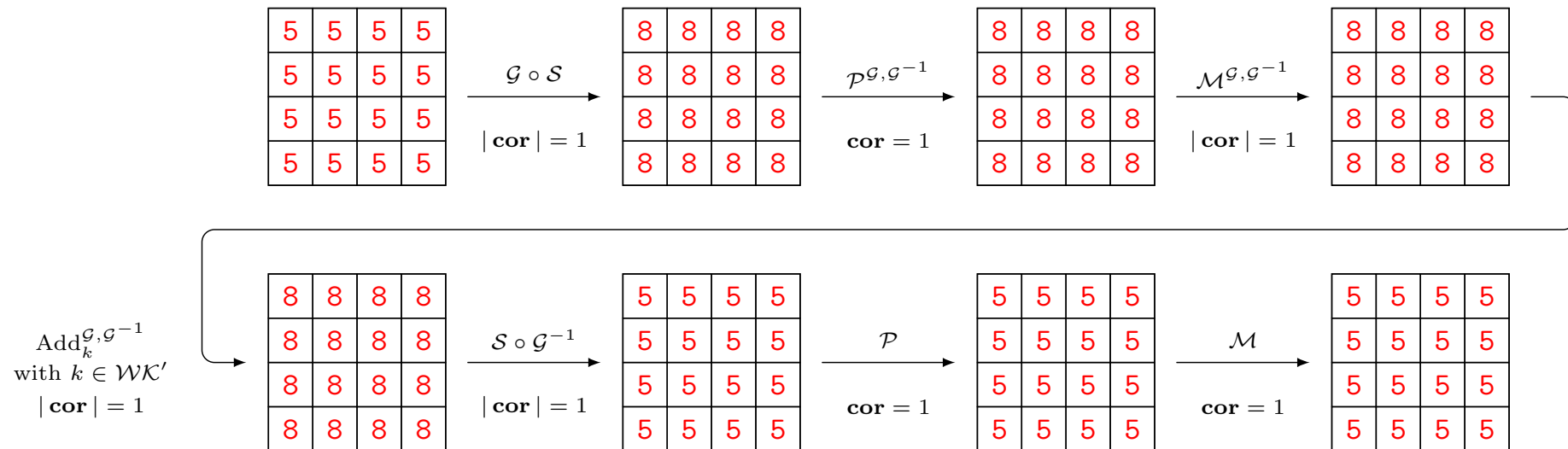
$$\text{cor}_S(\ell_\alpha, g) = \text{cor}_{G \circ S}(\alpha, 8) = -1 .$$

$$|\text{cor}_{\mathcal{M}^{g, g^{-1}}}((8, \dots, 8), (8, \dots, 8))| = 1 .$$

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 ± 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:

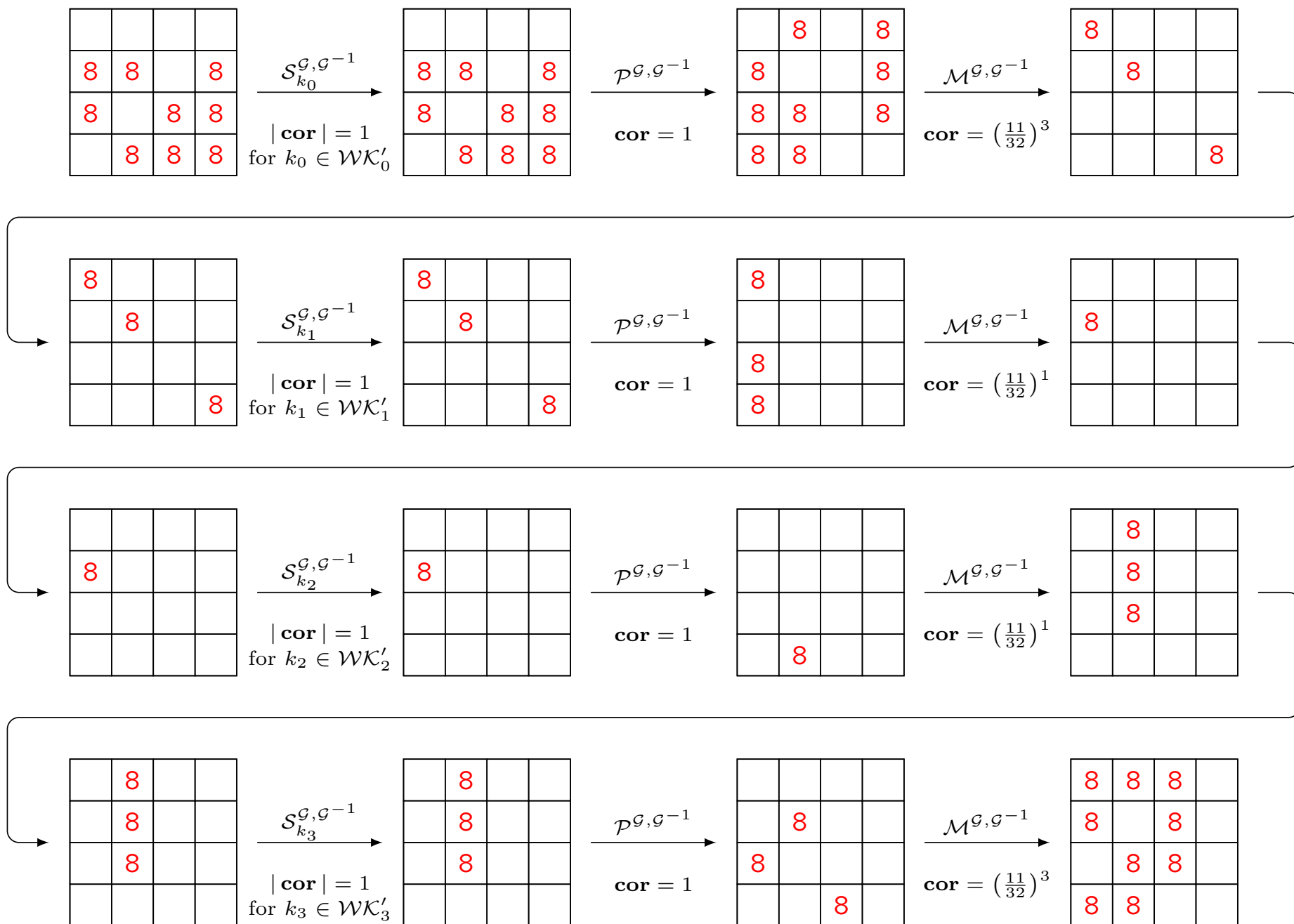
$$|\text{cor}_{SG, G^{-1}}(8, 8)| = 1 .$$

But,

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

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 0 or 1 in all active cells.

Correlation of the trail:

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

Correlation of the approximation:

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

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

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

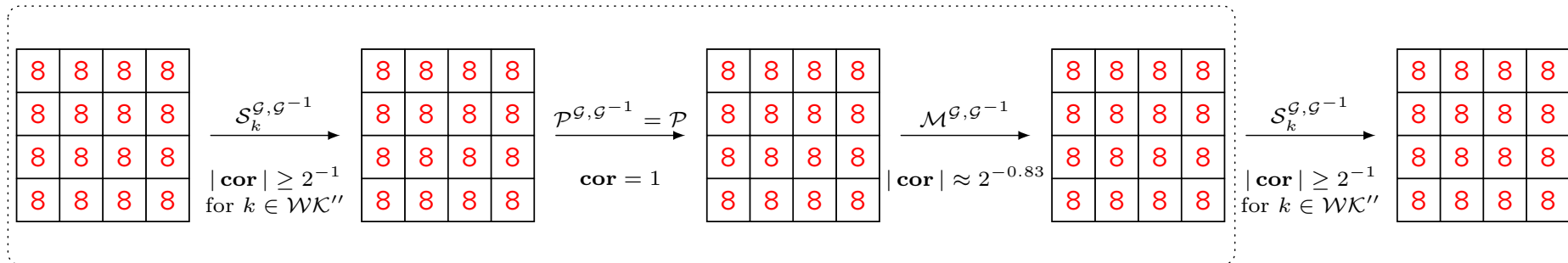
Another 1-round \mathcal{G} -shifted trail on Midori-64

$\mathcal{G} = (G', G, \dots, G)$ 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 $g'(x) = x_3x_2x_1 + x_3x_1 + x_3 + x_2 + x_1 + x_0$.

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

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

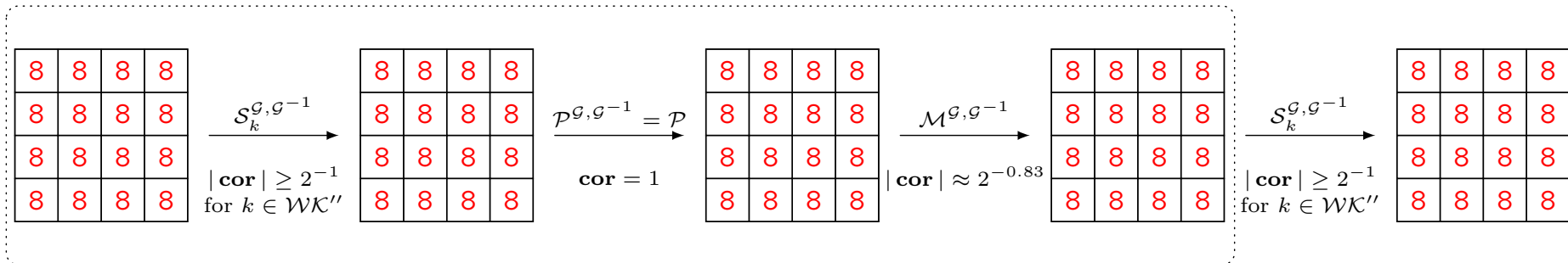
Another 1-round \mathcal{G} -shifted trail on Midori-64



Correlation of the 16-round trail:

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

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



Correlation of the 16-round trail:

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

Correlation over 16 rounds:

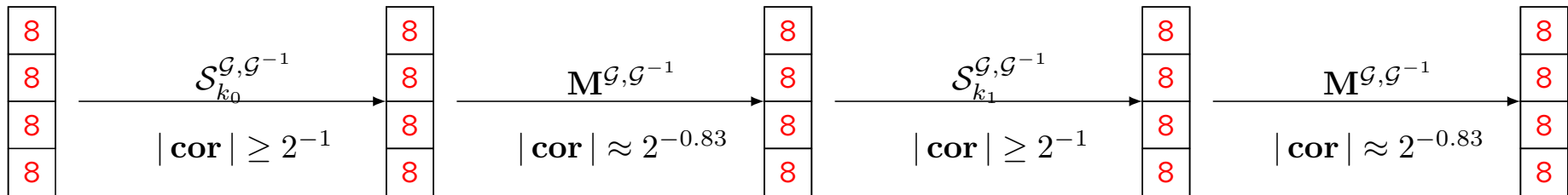
different from the correlation of the trail.

Focus on a single column

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

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

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



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

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

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?