Nonlinear Approximations in Cryptanalysis Revisited

Christof Beierle, Anne Canteaut and Gregor Leander

SnT, University of Luxembourg, Luxembourg
Inria, Paris, France
HGI, Ruhr-Universität Bochum, Germany

FSE 2019
Introduction

- Linear cryptanalysis [Matsui 94] as a standard attack method.
  - approximate linear function in the output by a linear function.

Generalization to nonlinear approximations was first discussed by Harpes, Kramer and Massey in 1995 and Knudsen, Robshaw in 1996. They were rediscovered in the context of invariant attacks, i.e., invariant subspace attacks [Leander et al. 2011] and the nonlinear invariant attack [Todo, Leander, Sasaki 2016].

Our Contribution

We study nonlinear approximations using the framework of linear cryptanalysis.
Introduction

- Linear cryptanalysis [Matsui 94] as a standard attack method.
  → approximate linear function in the output by a linear function.
- Generalization to nonlinear approximations was first discussed by Harpes, Kramer and Massey in 1995 and Knudsen, Robshaw in 1996.

Our Contribution
We study nonlinear approximations using the framework of linear cryptanalysis.
Introduction

- Linear cryptanalysis [Matsui 94] as a standard attack method. → approximate linear function in the output by a linear function.
- Generalization to nonlinear approximations was first discussed by Harpes, Kramer and Massey in 1995 and Knudsen, Robshaw in 1996.
- They were rediscovered in the context of invariant attacks, i.e., invariant subspace attacks [Leander et al. 2011] and the nonlinear invariant attack [Todo, Leander, Sasaki 2016]. → deterministic nonlinear approximations
Introduction

- Linear cryptanalysis [Matsui 94] as a standard attack method.
  → approximate linear function in the output by a linear function.

- Generalization to nonlinear approximations was first discussed by Harpes, Kramer and Massey in 1995 and Knudsen, Robshaw in 1996.

- They were rediscovered in the context of invariant attacks, i.e., invariant subspace attacks [Leander et al. 2011] and the nonlinear invariant attack [Todo, Leander, Sasaki 2016].
  → deterministic nonlinear approximations

Our Contribution

We study nonlinear approximations using the framework of linear cryptanalysis.
Outline

1. Our framework for (non-)linear approximations

2. Invariants imply highly-biased linear approximations (in many cases)

3. Probabilistic nonlinear approximations for cryptanalysis
(Non-)linear Approximations

- Let $F : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$ be a function (e.g., a block cipher with a fixed key).
- Approximate a Boolean function $h$ in the output by a Boolean function $g$ in the input.
- Quantify $\text{Prob}_x [g(x) + h(F(x)) = 0] - \frac{1}{2}$.
Let $F : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$ be a function (e.g., a block cipher with a fixed key).

Approximate a Boolean function $h$ in the output by a Boolean function $g$ in the input.

Quantify $\operatorname{Prob}_x [g(x) + h(F(x)) = 0] - \frac{1}{2}$

**Definition: Correlation of an Approximation**

Let $g : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$, $h : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be Boolean functions. The correlation of the approximation $g(x) \approx h(F(x))$ is defined as

$$\operatorname{cor}_F(g, h) := 2 \cdot \operatorname{Prob}_x [g(x) = h(F(x))] - 1.$$
(Non-)linear Approximations

- Let $F : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$ be a function (e.g., a block cipher with a fixed key)
- Approximate a Boolean function $h$ in the output by a Boolean function $g$ in the input
- Quantify $\text{Prob}_x [g(x) + h(F(x)) = 0] - \frac{1}{2}$

**Definition: Correlation of an Approximation**

Let $g : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$, $h : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be Boolean functions. The correlation of the approximation $g(x) \approx h(F(x))$ is defined as

$$\text{cor}_F(g, h) := 2 \cdot \text{Prob}_x [g(x) = h(F(x))] - 1.$$ 

Example: For $\gamma \in \mathbb{F}_2^n$, let $\ell_\gamma$ be the linear function defined by

$$\ell_\gamma : \mathbb{F}_2^n \rightarrow \mathbb{F}_2, x \mapsto \langle \gamma, x \rangle.$$ 

Linear cryptanalysis exploits the existence of $\gamma, \gamma' \in \mathbb{F}_2^n$ for which

$$|\text{cor}_{E_k}(\ell_\gamma, \ell_{\gamma'})| \gg 2^{-\frac{n}{2}}.$$
(Nonlinear) Invariant Attacks [Todo, Leander, Sasaki 2016]

**Definition: Invariant Set**

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation. $S \subseteq \mathbb{F}_2^n$ is an invariant set for $F$ if $F(S) = S$ or $F(S) = \mathbb{F}_2^n \setminus S$. 

Equivalently:

Let $g$ be the $n$-bit Boolean function defined by $g(x) := 1$ iff $x \in S$. Then, $orall x \in \mathbb{F}_2^n$: $g(F(x)) = g(x)$ or $orall x \in \mathbb{F}_2^n$: $g(F(x)) = g(x) + 1$. 

Correlation of an invariant $\text{cor}(F(g, g)) \in \{\pm 1\}$. 

Beierle, Canteaut, Leander

Nonlinear Approximations Revisited

FSE 2019
(Nonlinear) Invariant Attacks [Todo, Leander, Sasaki 2016]

Definition: Invariant Set

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation. $S \subseteq \mathbb{F}_2^n$ is an invariant set for $F$ if $F(S) = S$ or $F(S) = \mathbb{F}_2^n \setminus S$. 

Equivalently:

Let $g$ be the $n$-bit Boolean function defined by $g(x) := 1$ iff $x \in S$. Then, $\forall x \in \mathbb{F}_2^n: g(F(x)) = g(x)$ or $\forall x \in \mathbb{F}_2^n: g(F(x)) = g(x) + 1$.

Correlation of an invariant $\text{cor}_{F}(g, g) \in \{\pm 1\}$
**Definition: Invariant Set**

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation. $S \subseteq \mathbb{F}_2^n$ is an **invariant set** for $F$ if $F(S) = S$ or $F(S) = \mathbb{F}_2^n \setminus S$.

**Equivalently:**

Let $g$ be the $n$-bit Boolean function defined by $g(x) := 1$ iff $x \in S$. Then,

$$\forall x \in \mathbb{F}_2^n : g(F(x)) = g(x) \text{ or } \forall x \in \mathbb{F}_2^n : g(F(x)) = g(x) + 1.$$
**Definition: Invariant Set**

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation. $S \subseteq \mathbb{F}_2^n$ is an invariant set for $F$ if $F(S) = S$ or $F(S) = \mathbb{F}_2^n \setminus S$.

**Equivalently:**

Let $g$ be the $n$-bit Boolean function defined by $g(x) := 1$ iff $x \in S$. Then,

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

**Correlation of an invariant**

$$\text{cor}_F(g, g) \in \{\pm 1\}$$
Thm: Linear Trail Composition [Daemen, Govaerts, Vandewalle 1995]

Let $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be of the form $F = F_t \circ \cdots \circ F_1$ with $F_i: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. The correlation of an approximation $\ell_{\alpha_0}(x) \approx \ell_{\alpha_t}(F(x))$ can be given as

$$\text{cor}_F(\ell_{\alpha_0}, \ell_{\alpha_t}) = \sum_{\alpha_1, \ldots, \alpha_{t-1} \in \mathbb{F}_2^n} \prod_{i=1}^t \text{cor}_{F_i}(\ell_{\alpha_{i-1}}, \ell_{\alpha_i}).$$
**Thm: Linear Trail Composition [Daemen, Govaerts, Vandewalle 1995]**

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be of the form $F = F_t \circ \cdots \circ F_1$ with $F_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$. The correlation of an approximation $\ell_{\alpha_0}(x) \approx \ell_{\alpha_t}(F(x))$ can be given as

$$
cor_F(\ell_{\alpha_0}, \ell_{\alpha_t}) = \sum_{\alpha_1, \ldots, \alpha_{t-1} \in \mathbb{F}_2^n} \prod_{i=1}^{t} cor_{F_i}(\ell_{\alpha_{i-1}}, \ell_{\alpha_i}).$$

**Thm: Nonlinear Trail Composition**

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let $g, h : \mathbb{F}_2^n \to \mathbb{F}_2$. Then,

$$
cor_F(g, h) = \sum_{\gamma, \gamma' \in \mathbb{F}_2^n} cor_g(\ell_{\gamma}) cor_F(\ell_{\gamma}, \ell_{\gamma'}) cor_h(\ell_{\gamma'}),$$

where $cor_g(\ell_{\gamma}) := cor_g(\ell_{\gamma}, 1) = 2 \text{Prob}_x(\langle \gamma, x \rangle = g(x)) - 1$. 

Outline

1. Our framework for (non-)linear approximations
2. Invariants imply highly-biased linear approximations (in many cases)
3. Probabilistic nonlinear approximations for cryptanalysis
Thm: Nonlinear Trail Composition

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let $g, h : \mathbb{F}_2^n \to \mathbb{F}_2$. Then,

$$
cor_F(g, h) = \sum_{\gamma, \gamma' \in \mathbb{F}_2^n} cor_g(\ell_\gamma) \cdot cor_F(\ell_\gamma, \ell_{\gamma'}) \cdot cor_h(\ell_{\gamma'}) ,
$$

where $cor_g(\ell_\gamma) := cor_g(\ell_\gamma, \ell_1) = 2 \text{Prob}_x(\langle \gamma, x \rangle = g(x)) - 1$. 

Thm: Nonlinear Trail Composition

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let $g, h : \mathbb{F}_2^n \to \mathbb{F}_2$. Then,

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

where $\text{cor}_g(\ell_{\gamma}) := \text{cor}_g(\ell_{\gamma}, \ell_1) = 2 \Pr_X(\langle \gamma, x \rangle = g(x)) - 1$.

Let $g$ be an invariant for a permutation $F$. We obtain

$$1 = |\text{cor}_F(g, g)|$$
Representing Invariants as a Nonlinear Approximation

**Thm: Nonlinear Trail Composition**

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let $g, h : \mathbb{F}_2^n \to \mathbb{F}_2$. Then,

$$
cor_F(g, h) = \sum_{\gamma, \gamma' \in \mathbb{F}_2^n} cor_g(\ell_\gamma) cor_F(\ell_\gamma, \ell_{\gamma'}) cor_h(\ell_{\gamma'}) ,
$$

where $cor_g(\ell_\gamma) := cor_g(\ell_\gamma, \ell_1) = 2 \text{Prob}_x(\langle \gamma, x \rangle = g(x)) - 1$.

Let $g$ be an invariant for a permutation $F$. We obtain

$$
1 = | cor_F(g, g) | = | \sum_{\gamma, \gamma' \in \Gamma_g} cor_g(\ell_\gamma) cor_F(\ell_\gamma, \ell_{\gamma'}) cor_g(\ell_{\gamma'}) | ,
$$

where $\Gamma_g := \{ \gamma | cor_g(\ell_\gamma) \neq 0 \}$. 


BPF: A balanced Boolean function $g$ such that, $\forall \gamma: \text{cor}_g(\ell_\gamma) \in \{0, \pm L\}$

**Thm: Existence of Highly-Biased Linear Approximations (1)**

Let $g$ be a BPF which is invariant for a permutation $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$. Then, there exists an $n$-bit Boolean function $f$ such that

$$\left| \sum_{\gamma, \gamma' \in \Gamma_g} (-1)^{f(\gamma)+f(\gamma')} \text{cor}_F(\ell_\gamma, \ell_{\gamma'}) \right| = |\Gamma_g|$$

Moreover, there exist nonzero $\gamma, \gamma'$ such that $|\text{cor}_F(\ell_\gamma, \ell_{\gamma'})| \geq \frac{1}{|\Gamma_g|}$.
The case of balanced plateaued functions (BPF)

BPF: A balanced Boolean function $g$ such that, $\forall \gamma: \text{cor}_g(\ell_\gamma) \in \{0, \pm L\}$

**Thm: Existence of Highly-Biased Linear Approximations (1)**

Let $g$ be a BPF which is invariant for a permutation $F: \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then, there exists an $n$-bit Boolean function $f$ such that

$$\left| \sum_{\gamma, \gamma' \in \Gamma_g} (-1)^{f(\gamma)+f(\gamma')} \text{cor}_F(\ell_\gamma, \ell_{\gamma'}) \right| = |\Gamma_g|$$

Moreover, there exist nonzero $\gamma, \gamma'$ such that $|\text{cor}_F(\ell_\gamma, \ell_{\gamma'})| \geq \frac{1}{|\Gamma_g|}$.

If $g$ is a quadratic Boolean function, then

$$\text{cor}_g(\ell_\gamma) \in \{0, \pm 2^{\frac{\dim \text{LS}(g) - n}{2}}\}.$$
Ex: Nonlinear invariant attack on SCREAM [TLS 2016]

- It is $n = 128$. Let $g$ be the quadratic invariant. There are $2^{96}$ weak keys.
It is $n = 128$. Let $g$ be the quadratic invariant. There are $2^{96}$ weak keys.

For each weak key $k$, there exists a Boolean function $f$ such that

$$\left| \sum_{\gamma, \gamma' \in \Gamma_g} (-1)^{f(\gamma)+f(\gamma')} \text{cor}_{E_k}(l_\gamma, l_{\gamma'}) \right| = |\Gamma_g| = 2^{32}.$$
It is $n = 128$. Let $g$ be the quadratic invariant. There are $2^{96}$ weak keys.

For each weak key $k$, there exists a Boolean function $f$ such that

$$\left| \sum_{\gamma, \gamma' \in \Gamma_g} (-1)^{f(\gamma)+f(\gamma')} \operatorname{cor}_{E_k}(\ell_\gamma, \ell_{\gamma'}) \right| = |\Gamma_g| = 2^{32}.$$ 

This implies, that for each weak key $k$, there exist a linear approximation $\ell_\gamma(x) \approx \ell_{\gamma'}(E_k(x))$ with

$$\left| \operatorname{cor}_{E_k}(\ell_\gamma, \ell_{\gamma'}) \right| \geq 2^{-32} \gg 2^{-\frac{n}{2}}$$
It is $n = 128$. Let $g$ be the quadratic invariant. There are $2^{96}$ weak keys.

For each weak key $k$, there exists a Boolean function $f$ such that

$$\left| \sum_{\gamma, \gamma' \in \Gamma_g} (-1)^{f(\gamma) + f(\gamma')} \text{cor}_{E_k}(\ell_\gamma, \ell_{\gamma'}) \right| = |\Gamma_g| = 2^{32}.$$ 

This implies, that for each weak key $k$, there exist a linear approximation $\ell_\gamma(x) \approx \ell_{\gamma'}(E_k(x))$ with

$$|\text{cor}_{E_k}(\ell_\gamma, \ell_{\gamma'})| \geq 2^{-32} \gg 2^{-\frac{n}{2}}$$

Since $g$ is invariant for each of the rounds, the existence of this linear approximation is independent on the number of rounds!
The case of invariant subspaces

Invariant subspace attack: \( g \) is the indicator function of an affine subspace

**Thm: Existence of Highly-Biased Linear Approximations (2)**

Let \((U + a) \subseteq \mathbb{F}_2^n\) be an invariant affine subspace for a permutation \( F \). Then, for any nonzero \( \gamma' \in U^\perp \), there exists a \( \gamma \in U^\perp \setminus \{0\} \) such that

\[
|\text{cor}_F(l_\gamma, l_{\gamma'})| \geq 2^{-n + \dim U}
\]

In 2011, Leander et al. already proved the existence of a linear approximation with

\[
|\text{cor}_F(l_\gamma, l_{\gamma'})| \geq 2^{-n + \dim U - 2^{-n + \dim U}}.
\]
The case of invariant subspaces

Invariant subspace attack: $g$ is the indicator function of an affine subspace

**Thm: Existence of Highly-Biased Linear Approximations (2)**

Let $(U + a) \subseteq \mathbb{F}_2^n$ be an invariant affine subspace for a permutation $F$. Then, for any nonzero $\gamma' \in U^\perp$, there exists a $\gamma \in U^\perp \setminus \{0\}$ such that

$$|\text{cor}_F(\ell_\gamma, \ell_{\gamma'})| \geq 2^{-n+\dim U}$$

In 2011, Leander et al. already proved the existence of a linear approximation with

$$|\text{cor}_F(\ell_\gamma, \ell_{\gamma'})| \geq 2^{-n+\dim U} - 2^{2(-n+\dim U)}.$$
Open Questions

- Can we say anything more about the highly-biased linear approximations besides their mere existence?
- In particular, can we understand more about the distribution of the correlations $\text{cor}_F(\ell_\gamma, \ell_{\gamma'})$ over all $\gamma, \gamma' \in \Gamma_g$?
1. Our framework for (non-)linear approximations

2. Invariants imply highly-biased linear approximations (in many cases)

3. Probabilistic nonlinear approximations for cryptanalysis
Nonlinear Cryptanalysis

The Goal

Express probabilistic nonlinear approximations in the framework of linear cryptanalysis.

Let $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation, let $g: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be balanced.

Construct a permutation $G: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ for which $g(x) = \langle \alpha, G(x) \rangle$.

We look at the transformed permutation $F_G, G^{-1} := G \circ F \circ G^{-1}$.

The approximation $g(x) \approx g(F(x))$ is the same as $\ell_\alpha(x) \approx \ell_\alpha(F_G, G^{-1}(x))$.

We can now use linear cryptanalysis over $F_G, G^{-1}$.\[\]
Nonlinear Cryptanalysis

The Goal
Express probabilistic nonlinear approximations in the framework of linear cryptanalysis.

The Idea
Instead of using nonlinear cryptanalysis over the cipher, we use linear cryptanalysis over a transformed version of the cipher.
Nonlinear Cryptanalysis

The Goal
Express probabilistic nonlinear approximations in the framework of linear cryptanalysis.

The Idea
Instead of using nonlinear cryptanalysis over the cipher, we use linear cryptanalysis over a transformed version of the cipher.

- let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation, let $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be balanced.
Nonlinear Cryptanalysis

The Goal
Express probabilistic nonlinear approximations in the framework of linear cryptanalysis.

The Idea
Instead of using nonlinear cryptanalysis over the cipher, we use linear cryptanalysis over a transformed version of the cipher.

- let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation, let $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be balanced.
- construct a permutation $\mathcal{G} : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ for which $g(x) = \langle \alpha, \mathcal{G}(x) \rangle$
Nonlinear Cryptanalysis

The Goal
Express probabilistic nonlinear approximations in the framework of linear cryptanalysis.

The Idea
Instead of using nonlinear cryptanalysis over the cipher, we use linear cryptanalysis over a transformed version of the cipher.

- let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation, let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be balanced.
- construct a permutation $\mathcal{G} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for which $g(x) = \langle \alpha, \mathcal{G}(x) \rangle$
- we look at the transformed permutation $F^{\mathcal{G},\mathcal{G}^{-1}} := \mathcal{G} \circ F \circ \mathcal{G}^{-1}$
Nonlinear Cryptanalysis

The Goal

Express probabilistic nonlinear approximations in the framework of linear cryptanalysis.

The Idea

Instead of using nonlinear cryptanalysis over the cipher, we use linear cryptanalysis over a transformed version of the cipher.

- let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation, let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be balanced.
- construct a permutation $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for which $g(x) = \langle \alpha, G(x) \rangle$
- we look at the transformed permutation $F^G, G^{-1} := G \circ F \circ G^{-1}$
- the approximation $g(x) \approx g(F(x))$ is the same as $\ell_\alpha(x) \approx \ell_\alpha(F^G, G^{-1}(x))$
Nonlinear Cryptanalysis

The Goal
Express probabilistic nonlinear approximations in the framework of linear cryptanalysis.

The Idea
Instead of using nonlinear cryptanalysis over the cipher, we use linear cryptanalysis over a transformed version of the cipher.

- let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation, let $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be balanced.
- construct a permutation $G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ for which $g(x) = \langle \alpha, G(x) \rangle$
- we look at the transformed permutation $F^G,G^{-1} := G \circ F \circ G^{-1}$
- the approximation $g(x) \approx g(F(x))$ is the same as $\ell_\alpha(x) \approx \ell_\alpha(F^G,G^{-1}(x))$
- we can now use linear cryptanalysis over $F^G,G^{-1}$
as typical for linear cryptanalysis, we consider linear trails
as typical for linear cryptanalysis, we consider linear trails

if $E_k = R_{k_t} \circ \cdots \circ R_{k_1}$, then $E_k^{G,G^{-1}} = R_{k_t}^{G,G^{-1}} \circ \cdots \circ R_{k_1}^{G,G^{-1}}$
as typical for linear cryptanalysis, we consider linear trails

if $E_k = R_{k_t} \circ \cdots \circ R_{k_1}$, then $E_k^{G,G^{-1}} = R_{k_t}^{G,G^{-1}} \circ \cdots \circ R_{k_1}^{G,G^{-1}}$

we have

$$\text{cor}_{E_k^{G,G^{-1}}} (\ell_{\alpha_0}, \ell_{\alpha_t}) = \sum_{\alpha_1, \ldots, \alpha_{t-1} \in \mathbb{F}_2^n} \prod_{i=1}^{t} \text{cor}_{R_{k_i}^{G,G^{-1}}} (\ell_{\alpha_{i-1}}, \ell_{\alpha_i})$$
as typical for linear cryptanalysis, we consider linear trails

if \( E_k = R_{k_t} \circ \cdots \circ R_{k_1} \), then \( E_{k}^{G,G^{-1}} = R_{k_t}^{G,G^{-1}} \circ \cdots \circ R_{k_1}^{G,G^{-1}} \)

we have

\[
\text{cor}_{E_{k}^{G,G^{-1}}} (\ell_{\alpha_0}, \ell_{\alpha_t}) = \sum_{\alpha_1, \ldots, \alpha_{t-1} \in \mathbb{F}_2^n} \prod_{i=1}^{t} \text{cor}_{R_{k_i}^{G,G^{-1}}} (\ell_{\alpha_{i-1}}, \ell_{\alpha_i})
\]

we base the analysis on a single linear trail \((\alpha_0, \alpha_1, \ldots, \alpha_t)\) with correlation \( \prod_{i=1}^{t} \text{cor}_{R_{k_i}^{G,G^{-1}}} (\ell_{\alpha_{i-1}}, \ell_{\alpha_i}) \)
The linear trail corresponding to the invariant attack

Example: The invariant attack on Midori64 [Todo, Leander, Sasaki, 2016]
The linear trail corresponding to the invariant attack

Example: The invariant attack on Midori64 [Todo, Leander, Sasaki, 2016]

- let $S$ denote the S-box layer, i.e., a 16-times parallel application of the 4-bit S-box $S_b$. Let $S_k: x \mapsto S(x + k)$
The linear trail corresponding to the invariant attack

Example: The invariant attack on Midori64 [Todo, Leander, Sasaki, 2016]

- let $S$ denote the S-box layer, i.e., a 16-times parallel application of the 4-bit S-box $S_b$. Let $S_k : x \mapsto S(x + k)$
- $g(x) = x_3x_2 + x_2 + x_1 + x_0$ is used as an invariant for $S_b$. Weak keys are $(0, 0, *, *)$. 
The linear trail corresponding to the invariant attack

Example: The invariant attack on Midori64 [Todo, Leander, Sasaki, 2016]

- let \( S \) denote the S-box layer, i.e., a 16-times parallel application of the 4-bit S-box \( S_b \). Let \( S_k : x \mapsto S(x + k) \)
- \( g(x) = x_3x_2 + x_2 + x_1 + x_0 \) is used as an invariant for \( S_b \). Weak keys are \((0, 0, *, *)\).
- choose a permutation \( G : \mathbb{F}_2^4 \to \mathbb{F}_2^4 \) with \( g(x) = \langle 8, G(x) \rangle \) and define \( G := (G, G, \ldots, G) \)
The linear trail corresponding to the invariant attack

Example: The invariant attack on Midori64 [Todo, Leander, Sasaki, 2016]

- Let $S$ denote the S-box layer, i.e., a 16-times parallel application of the 4-bit S-box $S_b$. Let $S_k : x \mapsto S(x + k)$
- $g(x) = x_3 x_2 + x_2 + x_1 + x_0$ is used as an invariant for $S_b$. Weak keys are $(0, 0, *, *)$.
- Choose a permutation $G : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^4$ with $g(x) = \langle 8, G(x) \rangle$ and define $G := (G, G, \ldots, G)$

In this view, all S-boxes are active
we choose another (balanced) invariant for the S-box, i.e.,
\[ g'(x) = x_3 x_2 x_1 + x_3 x_1 + x_3 + x_2 + x_1 + x_0 \]
A Four-Round Linear Trail for transformed Midori64

- we choose another (balanced) invariant for the S-box, i.e.,
  \[ g'(x) = x_3 x_2 x_1 + x_3 x_1 + x_3 + x_2 + x_1 + x_0 \]
- choose \( G' : \mathbb{F}_2^4 \to \mathbb{F}_2^4 \) with \( g'(x) = \langle 8, G'(x) \rangle \), define \( G' := (G', \ldots, G') \)
we choose another (balanced) invariant for the S-box, i.e.,
\[ g'(x) = x_3x_2x_1 + x_3x_1 + x_3 + x_2 + x_1 + x_0 \]
choose \( G' : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^4 \) with \( g'(x) = \langle 8, G'(x) \rangle \), define \( G' := (G', \ldots, G') \)

we omit the key-schedule of Midori64 and assume independent round keys!
A Four-Round Linear Trail for transformed Midori64

\[ S_{G',G'-1}^{k_0} | \text{cor} | = 1 \quad \text{for } k_0 \in WK'_0 \]
\[ S_{k_1}^{G',G'-1} | \text{cor} | = 1 \quad \text{for } k_1 \in WK'_1 \]
\[ S_{k_2}^{G',G'-1} | \text{cor} | = 1 \quad \text{for } k_2 \in WK'_2 \]
\[ S_{k_3}^{G',G'-1} | \text{cor} | = 1 \quad \text{for } k_3 \in WK'_3 \]
if we use independent round keys in each round, $2^{208}$ out of all possible $2^{256}$ keys are weak

as the absolute correlation of the linear trail, we obtain $|\text{cor}| = 2^{-12.325}$

by experiments, we obtain $2^{-12.16}$ for the absolute correlation of the approximation using $2^{32}$ randomly chosen plaintexts
if we use independent round keys in each round, $2^{208}$ out of all possible $2^{256}$ keys are weak

as the absolute correlation of the linear trail, we obtain $|\text{cor}| = 2^{-12.325}$

by experiments, we obtain $2^{-12.16}$ for the absolute correlation of the approximation using $2^{32}$ randomly chosen plaintexts

but

by the wide-trail strategy, we expect $|\text{cor}| \geq 2^{-16}$ as the correlation of a four-round linear trail (16 active S-boxes)
we now use a probabilistic nonlinear approximation for the S-box layer
Another Linear Trail for transformed Midori64

- we now use a probabilistic nonlinear approximation for the S-box layer
- use the bijection $G'' := (G', G, \ldots, G)$ with
  \[ \langle 8, G(x) \rangle = x_3x_2 + x_2 + x_1 + x_0 \text{ (invariant for } S) \],
  \[ \langle 8, G'(x) \rangle = x_3x_2x_1 + x_3x_1 + x_3 + x_2 + x_1 + x_0. \]

Then

\[
\left| \text{cor}_{S_{k,G',G^{-1}}}(\ell_8, \ell_8) \right| = \begin{cases} 
1 & \text{if } k \in \{(0, 0, 0, \ast)\} \\
\frac{1}{2} & \text{else}
\end{cases}
\]
we now use a probabilistic nonlinear approximation for the S-box layer

use the bijection \( \mathcal{G}'' := (G', G, \ldots, G) \) with

\[
\langle 8, G(x) \rangle = x_3x_2 + x_2 + x_1 + x_0 \text{ (invariant for } S),
\]

\[
\langle 8, G'(x) \rangle = x_3x_2x_1 + x_3x_1 + x_3 + x_2 + x_1 + x_0. \text{ Then}
\]

\[
|\text{cor}_{S_{k}^{G', G'-1}}(\ell_8, \ell_8)| = \begin{cases} 1 & \text{if } k \in \{(0, 0, 0, \ast)\} \\ 1/2 & \text{else} \end{cases}
\]

\[
|\text{cor}_{S_{k}^{G'', G''-1}}(\ell_8, \ell_8)| \geq 2^{-1} \text{ for } k \in \mathcal{W}K''
\]

Correlation of the full-round trail is \( \geq (2^{-1.83})^{16} = 2^{-29.28} \).

but..
A Strong Linear-Hull Effect

The trail correlation does not approximate the correlation of the approximation!

Ex: Single column

Let $\tilde{G} = (G', G, G, G)$.

\[
\begin{array}{cccc}
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
\end{array}
\xrightarrow{S_{k_0}^{\tilde{G}, \tilde{G}^{-1}}} 
\begin{array}{cccc}
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
\end{array}
\xrightarrow{M_{\tilde{G}, \tilde{G}^{-1}}} 
\begin{array}{cccc}
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
\end{array}
\xrightarrow{S_{k_1}^{\tilde{G}, \tilde{G}^{-1}}} 
\begin{array}{cccc}
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
\end{array}
\xrightarrow{M_{\tilde{G}, \tilde{G}^{-1}}} 
\begin{array}{cccc}
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 \\
\end{array}
\]

If $k_0 \in \mathbb{F}_2^4 \times \{(0, 0, *, *)\}^3$ and $k_1 \in (\mathbb{F}_2^4 \setminus \{(0, 0, *, *)\}) \times \{(0, 0, *, *)\}^3$, then

$$\text{cor} R_{k_1} \circ R_{k_0} \left(\ell(8,8,8,8), \ell(8,8,8,8)\right) = 0$$
Open questions?

- In which cases can we approximate the approximation with a single trail?
- From another view: Can we use nonlinear approximations to quantify linear-hull effects in general?
Open questions?

- In which cases can we approximate the approximation with a single trail?
- From another view: Can we use nonlinear approximations to quantify linear-hull effects in general?

Thanks for your attention! Any questions?