Nonlinear Approximations in Cryptanalysis Revisited

Christof Beierle, Anne Canteaut, Gregor Leander

Nonlinear Approximations in Cryptanalysis Revisited

Christof Beierle[1], Anne Canteaut[2] and Gregor Leander[3]

[1] SnT, University of Luxembourg, Luxembourg
beierle.christof@gmail.com
[2] Inria, Paris, France
anne.canteaut@inria.fr
[3] Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany
gregor.leander@rub.de

Abstract. This work studies deterministic and non-deterministic nonlinear approximations for cryptanalysis of block ciphers and cryptographic permutations and embeds it into the well-understood framework of linear cryptanalysis. For a deterministic (i.e., with correlation ± 1) nonlinear approximation we show that in many cases, such a nonlinear approximation implies the existence of a highly-biased linear approximation. For non-deterministic nonlinear approximations, by transforming the cipher under consideration by conjugating each keyed instance with a fixed permutation, we are able to transfer many methods from linear cryptanalysis to the nonlinear case. Using this framework we in particular show that there exist ciphers for which some transformed versions are significantly weaker with regard to linear cryptanalysis than their original counterparts.

Keywords: Block cipher · Nonlinear invariant · Invariant subspace attack · Nonlinear approximations · Linear cryptanalysis · Midori

1 Introduction

Block ciphers are certainly among the most important cryptographic primitives when measured in terms of actual usage in practice. Luckily, ever since the development of the Advanced Encryption Standard (AES) we have at our disposal an efficient block cipher that withstood a significant amount of cryptanalytic efforts. Indeed, at least in the single-user scenario, breaking even the smallest variant of AES with a 128-bit key is still completely out of reach.

However, as the security of any block cipher is always inherently the security against known attacks, it is still an important task to investigate new ways of trying to tackle the security of those ciphers. Two current trends in symmetric cryptography stimulate this development of new attacks and the gain of fundamental new insights.

Firstly, within the last 10 years we have witnessed the emerging of many new ciphers aiming for execution under extreme performance constraints, often summarized as so-called *lightweight cryptography*. Besides the obvious contribution, one major impact of those new designs was that suddenly many new and interesting targets for new cryptanalytic attacks were available. Indeed, due to the sharp performance constraints, designs in the area of lightweight cryptography tend to be minimized with respect to their security margin and to be maximized with respect to simplicity. This has actually led to many designs being broken. While in some cases the new designs could be broken with (slightly modified) standard attacks, we have also seen new attack ideas being developed and some old attacks, that have been partially forgotten, have found new applications.

IACR Transactions on Symmetric Cryptology ISSN 2519-173X, Vol. 2018, No. 4, pp. 80–101
DOI:10.13154/tosc.v2018.i4.80-101

A second, and more recent, trend in symmetric cryptography that can be identified is the focus on so-called cryptographic permutations as very versatile tools. Instead of a block cipher, that is a family of permutations, it turns out that in many cases it is enough to design only one permutation and use it within a suitable mode of operation. Important examples include Keccak (and more generally the Sponge construction) and many recent authenticated encryption designs, see e.g. the CAESAR competition. An even more recent interesting example is the Farfalle construction [BDH+17].

Even though a cryptographic permutation and a block cipher are conceptually very different objects, it is worth noticing that the design and analysis of both primitives is very related in practice. Indeed, many cryptographic permutations are analyzed with respect to differential and linear cryptanalysis just as block ciphers are. While the design of cryptographic permutations gives significantly more freedom to the designer (especially in modes where the inverse is not required), for the cryptanalytic scope of our work, cryptographic permutations can be seen as *block ciphers with a fixed key*.

When it comes to new attack vectors, a line of work we like to highlight here is the class of *invariant attacks*. In a nutshell, those attacks make use of a partition of the plaintexts into two sets such that, for some keys, this partitioning is invariant under encryption. Keys for which this partitioning is invariant are called *weak keys*. The attack started with the case where the partitioning of the plaintext space was with respect to an affine subspace and its complement [LAAZ11] and was later generalized to sets of different form (see [TLS16]). An important detail to point out here is that the partitioning was found using the iterative structure of virtually all modern block ciphers and cryptographic permutations. Instead of finding the partition for the whole cipher or permutation directly, all known attacks of this type find an invariant for a single round, or at most two rounds as in the recent work [Bey18], and extend those for the whole cipher by induction.

Those two important restrictions, namely a partition that is invariant, i.e., works with probability one and that the partitioning is invariant for all rounds actually implies that those attacks, if existent, can be efficiently detected. Even more, under some constraints, one can even exclude their existence efficiently. As we will discuss below, invariant subspace attacks and nonlinear invariant attacks can be seen as special cases of attacks that have been known for much longer. However, those attacks had the significant drawback of being either too general or of having not enough suitable targets, i.e. block ciphers, at the time of invention.

However, while those restrictions mentioned above were key to those attacks being applicable, they immediately lead to many questions to be answered. In particular, directly related to the two restrictions above, one could investigate how to allow those invariants to hold with a non trivial probability only, i.e. non-linear approximations. Answering this question clearly has the ability to give insights significantly improving upon the state of the art. In particular, this line of research can be expected to shed more light on the design of cryptographic permutations and the round constants for those.

The task here is to keep the generalization manageable and, in the optimal case, to link it to well-understood areas of symmetric cryptography.

Our Contribution

This work explores a link between linear cryptanalysis and nonlinear approximations. In this line, we address the open question mentioned above. Namely, for the case of partitions that hold with a non-trivial probability only, we establish several links to the well-understood framework of linear cryptanalysis. This allows us to apply some of the well-established theory for linear cryptanalysis to its nonlinear counterpart. In Section 2, we first recall the well-known cryptanalytic approach of approximating a Boolean function in the cipher's output by a Boolean function in the input, a method to which both linear cryptanalysis and invariant attacks belong as special cases. We recall how those two kinds

of attacks can be phrased in this unified framework.

In Section 3, we then first focus on *invariant attacks*, i.e., the invariant subspace attack and the nonlinear invariant attack, which utilize deterministic (nonlinear) approximations over keyed instances of the cipher for a particular set of weak keys. In this context, deterministic means that the approximation holds with an absolute correlation equal to 1. We show that a Boolean function $g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ which is an invariant for a keyed instance of the cipher gives rise to the existence of a highly-biased (non-trivial) linear approximation of the instance in many practical cases. In particular, such linear approximations can be guaranteed whenever g is either a balanced *plateaued function*, i.e., a balanced function for which there exists an L such that its Walsh spectrum is equal to $\{0, \pm L\}$, or an *indicator function of an affine subspace* of $\mathbb{F}_2^n$. As plateaued functions contain all Boolean functions of algebraic degree 2 as a subset, such highly-biased linear approximations can be guaranteed for the block ciphers Midori64 [BBI+15], SCREAM [GLS+15] and iSCREAM [GLS+14] when instantiated with a key from the set of weak keys according the nonlinear invariant attack, as described in [TLS16]. When g is the indicator function of an affine subspace $U + a \subseteq \mathbb{F}_2^n$ which is invariant for a keyed instance E_k of the cipher, we show that, for all output masks $\gamma' \in U^\perp \setminus \{0\}$, there exists a non-zero input mask γ for which $|\mathbf{cor}_{E_k}(\gamma, \gamma')| \geq 2^{-n+\dim U}$. This improves a result derived in [LAAZ11], where the existence of (only a single) linear approximation with correlation greater or equal to $2^{-n+\dim U} - 2^{2(-n+\dim U)}$ was shown. Similar as in [LAAZ11], our arguments are non-constructive and therefore, we are not able to identify those highly-biased linear approximations. Thus, we just state their existence. Although those approximations are key dependent, for any weak key, the existence of a linear approximation with a high bias might still contradict the designers' claims.

Section 4 deals with utilizing *probabilistic nonlinear approximations* for block cipher cryptanalysis. In particular, we propose a way to study nonlinear approximations in the better-understood framework of linear cryptanalysis. The basic idea is to embed the balanced nonlinear Boolean function g used for the approximation into one component function of a bijection $\mathcal{G}$ on n bits, where n denotes the block length of the cipher under consideration. The basic observation is that if the approximation $g(x) \approx g(E_k(x))$ holds with a high bias, the *transformed* cipher $\mathcal{G} \circ E_k \circ \mathcal{G}^{-1}$ could be approximated by the *linear approximation* $\langle \alpha, x\rangle \approx \langle \alpha, \mathcal{G} \circ E_k \circ \mathcal{G}^{-1}(x)\rangle$ holding with the same bias, where α determines the component of $\mathcal{G}$ that embeds g, i.e., $\langle \alpha, \mathcal{G}\rangle = g$.

As a case study, we consider the lightweight block cipher Midori64 [BBI+15]. We first express the nonlinear invariant attack in terms of a *linear trail over a transformed version of the cipher*. The nonlinear invariant attack could be viewed in terms of an invariant subspace of dimension $(n-1)$ over the transformed cipher. We then focus on probabilistic approximations and show an example on four rounds of Midori64 *with independent round keys*. In particular, we show the existence of a four-round linear trail over the transformed cipher with absolute correlation $2^{-12.3}$ for 2^{208} out of the 2^{256} possible keys. An important observation is that the absolute correlation of this four-round trail exceeds the highest possible absolute correlation of any four-round linear trail for the cipher which is upper-bounded by 2^{-16}. This implies that considering such a transformed version of the cipher may reveal unexpected vulnerabilities to linear cryptanalysis. We also exhibit another linear trail for the transformed version of Midori64 and we show that this trail cannot be used to estimate the correlation of the corresponding approximation due to a strong linear-hull effect.

Related Work

In 1993, Matsui introduced the technique of *linear cryptanalysis* [Mat94b]. The idea can be phrased as approximating a linear Boolean function in the cipher's output by a linear Boolean function in the input. Later in 1995 and 1996, the generalization of utilizing nonlinear approximations was discussed by Harpes, Kramer and Massey [HKM95] and

Knudsen and Robshaw [KR96]. The problems that come along with this generalization, i.e., the much larger search space compared to linear functions and a rather complex key dependency were already mentioned. Due to the work of Nyberg [Nyb95a] and Daemen, Govaerts and Vandewalle [DGV95] as well as Daemen and Rijmen [DR07] for the case of key-alternating ciphers, the technique of linear cryptanalysis and in particular the key dependency in linear approximations is quite well understood.

Attacks that are based on partitioning the message space in a way that the partition is preserved after encryption were already considered in the 90s' by Harpes and Massey [Har96, HM97] and Paterson [Pat99]. In [Har96, HM97], *partitioning cryptanalysis* was introduced as a generalization of Matsui's linear cryptanalysis. The attack exploits the weakness that there exists a large subset X of the input space and partitions $P = \{P_1, \ldots, P_\ell\}$ and $Q = \{Q_1, \ldots, Q_\ell\}$ of X such that each block of P is mapped to a block of Q under the encryption. In the special case of linear cryptanalysis, both partitions P and Q consist of a subset of a hyperplane and a subset of its complement. In [Pat99], the focus was on the case where the subset X is equal to the whole input space and the previous described property on preserving a partition holds for each round of an iterated cipher. Thus, the concept described in [Pat99] is closely related to the *invariant subspace attack* [LAAZ11, LMR15] and the *nonlinear invariant attack* [TLS16]. In [LAAZ11] it was shown that the lightweight cipher PRINTcipher exhibits the following weakness: There exists an affine subspace $(U + a)$ of the input space $\mathbb{F}_2^n$ such that, for many keys k, the affine space $(U + a)$ is invariant under the encryption with the key k. This attack has then been successfully applied to quite a number of recent designs including Midori64 [GJN+16], iSCREAM [LMR15], NORX v2.0 [CFG+17], Simpira v1 [Røn16] and Haraka v.0 [Jea16]. Moreover, some general design criteria on the S-box layer have been presented in [GJN+16] in order to prevent the existence of such invariant subspaces. In [TLS16], similar attacks in the weak key setting were constructed with the difference that, instead of an *affine subspace*, the partition of $\mathbb{F}_2^n$ into a *set* I and its complement is preserved under encryption with a weak key. Both of these attacks exploit the invariance for each round of the cipher separately. In [BCLR17], the authors show how one could protect lightweight substitution-permutation ciphers against such attacks by carefully choosing the round constants together with the linear layer.

Very recently, Beyne defined invariants in terms of eigenvectors of correlation matrices [Bey18]. For Midori64 with modified round constants, he derived an invariant (which admits a larger space of weak keys) which is *not invariant for a single round*, but two rounds instead. Moreover, he found a *linear invariant* for any even number of rounds for the modified version of Midori64, which corresponds to a linear approximation of maximum correlation ± 1.

2 Preliminaries

Let $n, \kappa > 1$ be positive integers. In this work, we consider a general block cipher

$$\begin{aligned} E\colon \mathbb{F}_2^n \times \mathbb{F}_2^\kappa &\to \mathbb{F}_2^n \\ (x, k) &\mapsto E(x, k)\ . \end{aligned}$$

By the definition of a block cipher, for each $k \in \mathbb{F}_2^\kappa$, the projection $E_k \coloneqq E(\cdot, k)$ is a permutation on $\mathbb{F}_2^n$. We will refer to n as the *block length*, κ as the *key length*, $k \in \mathbb{F}_2^\kappa$ as the *key*, and E_k as the *keyed instance* of the cipher for the key k.

For two arbitrary vectors $\alpha, x \in \mathbb{F}_2^n$, we denote the canonical inner product by $\langle \alpha, x \rangle \coloneqq \sum_i \alpha_i x_i \in \mathbb{F}_2$.

2.1 Approximations by Boolean Functions

In this work, we consider adversaries who aim at distinguishing a block cipher E from a family of permutations chosen uniformly at random. We consider the attack strategy of approximating a (non-constant) Boolean function of the output by a Boolean function of the input. In a nutshell, given two n-bit non-constant Boolean functions g and h with the same Hamming weight such that, for many keys k, the identity $g(x) = h(E_k(x))$ holds with a high absolute bias, i.e., for significantly more or significantly less than half of all $x \in \mathbb{F}_2^n$, one obtains a distinguisher by evaluating g and h on (many) known plaintext/ciphertext pairs (x, y), respectively. For a fixed keyed instance, the bias of such an approximation can be measured by its *correlation*, defined as follows.[1]

Definition 1 (Correlation of an Approximation)**.** Let $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^n$ be a vectorial function from m bits to n bits. For any Boolean functions $g\colon \mathbb{F}_2^m \to \mathbb{F}_2$ and $h\colon \mathbb{F}_2^n \to \mathbb{F}_2$, the *correlation* of the approximation $g(x) \approx h(F(x))$ is defined as

$$\mathbf{cor}_F(g, h) = 2^{-m} \sum_{x \in \mathbb{F}_2^m} (-1)^{g(x)+h(F(x))} \in [-1, 1] \,.$$

This general definition of the correlation of a (possibly nonlinear) approximation captures the notion of a (nonlinear) invariant for a cipher [TLS16]. Indeed, an *invariant* for an n-bit permutation F is defined as a set of inputs $I \subset \mathbb{F}_2^n$ which remains invariant under F (or which is mapped to its complement $\mathbb{F}_2^n \setminus I$). This equivalently means that the indicator function of I, i.e., the n-variable Boolean function g defined by $g(x) = 1$ if and only if $x \in I$, satisfies

$$\forall x \in \mathbb{F}_2^n\colon g(F(x)) = g(x) + \varepsilon$$

for a fixed $\varepsilon \in \mathbb{F}_2$. In other words, a set I is an invariant for F if and only if its indicator function g satisfies

$$|\,\mathbf{cor}_F(g, g)| = 1 \,.$$

2.2 Linear Cryptanalysis

Another special case of the above attack strategy is linear cryptanalysis [Mat94a, Mat94b], which restricts the choice of the Boolean functions g and h to linear functions. For a fixed n, the set of linear Boolean functions on n bits, denoted by $\mathcal{L}_n$, forms an $\mathbb{F}_2$-vector space of dimension n. In particular, there is a one-to-one correspondence between the elements in $\mathcal{L}_n$ and the elements in $\mathbb{F}_2^n$ as

$$\mathcal{L}_n \coloneqq \{\ell_\alpha\colon x \mapsto \langle \alpha, x\rangle \mid \alpha \in \mathbb{F}_2^n\} \,.$$

Whenever $\alpha \neq 0$, the corresponding linear function ℓ_α is balanced.

Therefore, in the framework of linear cryptanalysis, we consider an adversary who selects two elements $\alpha, \beta \in \mathbb{F}_2^n \setminus \{0\}$ (also called *masks*) and exploits the approximation $\langle \alpha, x\rangle \approx \langle \beta, E_k(x)\rangle$, which should hold with a high absolute correlation. For the sake of simplicity, the *correlation of a linear approximation* will often be denoted by replacing the involved linear functions by the corresponding masks: For $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^n$,

$$\mathbf{cor}_F(\alpha, \beta) \coloneqq \mathbf{cor}_F(\ell_\alpha, \ell_\beta), \text{ with } \alpha \in \mathbb{F}_2^m, \beta \in \mathbb{F}_2^n \,.$$

Most notably, when $n = 1$, i.e., when F is a Boolean function, we define

$$\mathbf{cor}_F(\alpha) \coloneqq \mathbf{cor}_F(\alpha, 1) \,.$$

[1] We would like to remark that the cryptographic relevance of the correlation value depends on the weights of g and h. If they are extremely unbalanced, the advantage of the corresponding distinguisher might be negligible. A similar situation occurs for extremely unbalanced nonlinear invariants.

It is worth noticing that the mapping $(\alpha, \beta) \mapsto \mathbf{cor}_F(\alpha, \beta)$ is the discrete Fourier transform, aka *Walsh transform*) of F (see e.g. [Nyb95b, Page 113]). Therefore, the set $\{\mathbf{cor}_F(\alpha, \beta), \alpha \in \mathbb{F}_2^m, \beta \in \mathbb{F}_2^n\}$ is known as the *Walsh spectrum* of F.

Computing the correlation over an n-bit function in general quickly becomes impractical as n increases. However, common ciphers are designed as round-iterated functions and we can make use of the notion of *linear trails*, defined as follows.

Definition 2 (Linear Trail (see [DGV95]))**.** Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an iterated function of the form $F = F_t \circ \cdots \circ F_2 \circ F_1$ with $F_i\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. Given $(t+1)$ vectors $\alpha_0, \ldots, \alpha_t \in \mathbb{F}_2^n$, the tuple $(\alpha_0, \ldots, \alpha_t)$ is said to be a *linear trail* over F and its correlation is defined as

$$\mathbf{cor}_{F_1,\ldots,F_t}(\alpha_0, \alpha_1, \ldots, \alpha_t) \coloneqq \prod_{i=1}^{t} \mathbf{cor}_{F_i}(\alpha_{i-1}, \alpha_i) \ .$$

This leads to the following important theorem for iterative functions, which was first stated in [DGV95].

Theorem 1 (Theorem of Linear Trail Composition)**.** *Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an iterated function of the form $F = F_t \circ \cdots \circ F_2 \circ F_1$ with $F_i\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then, the correlation of the linear approximation (α_0, α_t) over F is given by the sum of the correlations of all its constituent linear trails, i.e.,*

$$\mathbf{cor}_F(\alpha_0, \alpha_t) = \sum_{\alpha_1,\ldots,\alpha_{t-1} \in \mathbb{F}_2^n} \mathbf{cor}_{F_1,\ldots,F_t}(\alpha_0, \alpha_1, \ldots, \alpha_{t-1}, \alpha_t) \ .$$

For the building blocks of key-alternating ciphers we can easily compute the correlation of linear approximations according to the following, well-known, rules.

Theorem 2 (Correlation over the Building Blocks of Iterated Ciphers)**.** *We can express the correlation over a linear layer, a key addition, and an S-box layer as follows:*

- *Let $\mathcal{L} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a linear permutation. Then,*

$$\mathbf{cor}_{\mathcal{L}}(\alpha, \beta) = \begin{cases} 1 & \text{if } \alpha = \mathcal{L}^\top(\beta) \\ 0 & \text{otherwise} \end{cases} \ ,$$

  where $\mathcal{L}^\top$ denotes the transpose of $\mathcal{L}$.

- *Let $T_k : \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto x + k$ be the $\mathbb{F}_2$-addition of the round-key $k \in \mathbb{F}_2^n$. Then,*

$$\mathbf{cor}_{T_k}(\alpha, \beta) = \begin{cases} (-1)^{\langle \alpha, k \rangle} & \text{if } \alpha = \beta \\ 0 & \text{otherwise} \end{cases} \ .$$

- *Let $\mathcal{S} : (\mathbb{F}_2^b)^s \to (\mathbb{F}_2^b)^s$ be the s-time parallel application of a function $S : \mathbb{F}_2^b \to \mathbb{F}_2^b$. Then,*

$$\mathbf{cor}_{\mathcal{S}}(\alpha, \beta) = \prod_{i=0}^{s-1} \mathbf{cor}_S(\alpha_i, \beta_i) \ .$$

In the following, we consider E to be a key-alternating cipher which iterates the unkeyed round permutation $\mathcal{R}\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ for t times and applies the round-key addition T_{k_i} in-between:

$$E_{(k_0,\ldots,k_t)} = T_{k_t} \circ \mathcal{R} \circ T_{k_{t-1}} \circ \cdots \circ T_{k_1} \circ \mathcal{R} \circ T_{k_0} \ .$$

From the above facts, the correlation over a keyed instance for a fixed master key $k = (k_0, \ldots, k_t)$ can be computed as

$$\mathbf{cor}_{E_k}(\alpha, \beta) = \sum_{\gamma_1, \ldots, \gamma_{t-1} \in \mathbb{F}_2^n} (-1)^{\langle \gamma, k \rangle} \prod_{i=0}^{t-1} \mathbf{cor}_{\mathcal{R}}(\gamma_i, \gamma_{i+1}) \,, \tag{1}$$

where $\gamma_0 = \alpha, \gamma_t = \beta$ and $\gamma = (\gamma_0, \ldots, \gamma_t)$ is the linear trail defined by all the intermediate masks γ_i.

This equation is what is usually described as the *linear hull*. One can see that the absolute value of the correlation of each linear trail is independent of the actual key k. However, the correlation of the linear hull, i.e. the sum of the correlations of the constituent linear trails, depends on the key. As computing this sum is usually impractical, distinguishers (and security arguments) are often based on a single (or few) dominant linear trail(s). When there is no dominant trail, estimating the correlation is much harder and often based on heuristic arguments. However, nonlinear invariants and nonlinear approximations may provide a tool for capturing a linear-hull effect. This was already nicely illustrated by the linear approximation with correlation ± 1 recently exhibited by Beyne on a variant of Midori64 [Bey18, Section 5.3].

3 A Link between Invariants and Linear Approximations

In this section, we show that the existence of a (nonlinear) invariant in many practical cases, or the existence of an invariant subspace, is closely related to the existence of highly-biased linear approximations of the cipher. Besides invariant subspaces, our argument covers all balanced *plateaued invariants*, i.e., any balanced invariant for which there exists an L such that its Walsh spectrum is equal to $\{0, \pm L\}$. In particular, this covers any quadratic invariant as a special case. Our result is based on the following theorem. Note that parts of the results presented in this section already appeared in the PhD thesis [Bei18].

Theorem 3 (Nonlinear Trail Composition)**.** *Let $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let g, h be n-bit Boolean functions. Then,*

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

Proof. The proof is very similar to the proof of the theorem of linear trail composition. We first show that, for any $\gamma' \in \mathbb{F}_2^n$, $\sum_{\gamma \in \mathbb{F}_2^n} \mathbf{cor}_g(\gamma)\, \mathbf{cor}_F(\gamma, \gamma') = \mathbf{cor}_F(g, \ell_{\gamma'})$. Indeed,

$$\begin{aligned}
\sum_{\gamma \in \mathbb{F}_2^n} \mathbf{cor}_g(\gamma)\, \mathbf{cor}_F(\gamma, \gamma') &= \sum_{\gamma \in \mathbb{F}_2^n} \frac{1}{2^n} \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle \gamma, x \rangle + g(x)} \sum_{x' \in \mathbb{F}_2^n} (-1)^{\langle \gamma, x' \rangle + \langle \gamma', F(x') \rangle} \\
&= \frac{1}{2^n} \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} \sum_{x' \in \mathbb{F}_2^n} (-1)^{g(x) + \langle \gamma', F(x') \rangle} \sum_{\gamma \in \mathbb{F}_2^n} (-1)^{\langle \gamma, x + x' \rangle} \\
&= \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x) + \langle \gamma', F(x) \rangle} = \mathbf{cor}_F(g, \ell_{\gamma'}) \,.
\end{aligned}$$

Using the previous formula, we prove the result as follows:

$$\begin{aligned}
&\sum_{\gamma\in\mathbb{F}_2^n}\sum_{\gamma'\in\mathbb{F}_2^n}\mathbf{cor}_g(\gamma)\,\mathbf{cor}_F(\gamma,\gamma')\,\mathbf{cor}_h(\gamma')\\
&\quad=\sum_{\gamma'\in\mathbb{F}_2^n}\mathbf{cor}_h(\gamma')\sum_{\gamma\in\mathbb{F}_2^n}\mathbf{cor}_g(\gamma)\,\mathbf{cor}_F(\gamma,\gamma')\\
&\quad=\sum_{\gamma'\in\mathbb{F}_2^n}\mathbf{cor}_h(\gamma')\,\mathbf{cor}_F(g,\ell_{\gamma'})\\
&\quad=\frac{1}{2^n}\frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{x'\in\mathbb{F}_2^n}(-1)^{g(x')+h(x)}\sum_{\gamma'\in\mathbb{F}_2^n}(-1)^{\langle\gamma',x+F(x')\rangle}\\
&\quad=\frac{1}{2^n}\sum_{x'\in\mathbb{F}_2^n}(-1)^{g(x')+h(F(x'))}=\mathbf{cor}_F(g,h)\;.
\end{aligned}$$

□

3.1 Invariant Attacks and a Link to Linear Cryptanalysis

In invariant attacks, the adversary is interested in finding an n-bit non-constant Boolean function $g:\mathbb{F}_2^n\to\mathbb{F}_2$ for which there exist many keys k such that $\forall x: g(x)=g(E_k(x))+\varepsilon_k$ for some $\varepsilon_k\in\mathbb{F}_2$. Those keys are called *weak keys* for E. In other words, an invariant g defines a nonlinear approximation with absolute correlation one, i.e., $|\mathbf{cor}_{E_k}(g,g)|=1$. We can now make use of the above theorem about nonlinear approximations and obtain the following direct corollary.

Corollary 1. *Let $F:\mathbb{F}_2^n\to\mathbb{F}_2^n$ and $g:\mathbb{F}_2^n\to\mathbb{F}_2$. Then, g is an invariant for F if and only if*

$$\left|\sum_{\gamma,\gamma'\in\Gamma_g}\mathbf{cor}_g(\gamma)\,\mathbf{cor}_F(\gamma,\gamma')\,\mathbf{cor}_g(\gamma')\right|=1\;,$$

where $\Gamma_g=\{\gamma\in\mathbb{F}_2^n\mid\mathbf{cor}_g(\gamma)\neq 0\}$.

3.1.1 The Nonlinear Invariants in Midori64, SCREAM and iSCREAM

As examples, we consider the nonlinear invariant attacks on Midori64 [BBI+15], SCREAM [GLS+15] and iSCREAM [GLS+14], as presented in [TLS16]. In all three examples, the invariant Boolean function g consists of 16 parallel applications of a function q of degree 2 with $\mathbf{cor}_q(\alpha)\in\{0,\pm\frac{1}{2}\}$ for all α. It follows that the absolute value of $\mathbf{cor}_g(\gamma)$ is the same for all γ in Γ_g and equal to 2^{-16}. Thus, the above formula simplifies to

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

where f is an n-bit Boolean function, E_k is a keyed instance of the particular cipher with a weak key, and $|\Gamma_g|=2^{32}$. From Equation (2), we can deduce that, for each weak key, there must exist linear approximations (over the whole cipher, and in fact for all possible number of rounds) with absolute correlation at least 2^{-32}.

This observation can be generalized to all balanced plateaued invariants, i.e., to all balanced functions g such that, for all $\gamma\in\mathbb{F}_2^n$, $\mathbf{cor}_g(\gamma)\in\{0,\pm L\}$ for some L (see [ZZ99]). Plateaued functions include as a special case all Boolean functions of degree 2. Indeed,

it is well known (see e.g. Theorem 4 in [Car07]) that any n-variable Boolean function g of degree 2 satisfies $\mathbf{cor}_g(\gamma) \in \{0, \pm 2^{\frac{\dim \mathsf{LS}(g)-n}{2}}\}$, where $\mathsf{LS}(g) := \{a \in \mathbb{F}_2^n : x \mapsto g(x+a)+g(x) \text{ is constant}\}$.

We then derive the following theorem which holds in particular when g has degree 2.

Theorem 4. *Let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be a* balanced plateaued *function which is invariant for E_k. Then, there exists a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that*

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

Most notably, there exist $\gamma, \gamma' \in \mathbb{F}_2^n \setminus \{0\}$ such that

$$|\mathbf{cor}_{E_k}(\gamma,\gamma')| \geq \frac{1}{|\Gamma_g|} \ .$$

Proof. From Corollary 1, we obtain that

$$\left| \sum_{\gamma,\gamma' \in \Gamma_g} \mathbf{cor}_g(\gamma)\, \mathbf{cor}_g(\gamma')\, \mathbf{cor}_{E_k}(\gamma,\gamma') \right| = 1 \ ,$$

where $\Gamma_g = \{\gamma \in \mathbb{F}_2^n | \, \mathbf{cor}_g(\gamma) \neq 0\}$. Since there exists an L such that $\mathbf{cor}_g(\gamma) = \pm L$ for all $\gamma \in \Gamma_g$, we derive that

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

for an appropriate function f that takes care of the sign. Moreover, Parseval's relation implies that

$$\sum_{\gamma \in \Gamma_g} \mathbf{cor}_g(\gamma)^2 = |\Gamma_g| L^2 = 1 \ ,$$

leading to $|\Gamma_g| = L^{-2}$. We deduce that

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

The existence of a pair $(\gamma, \gamma') \in \Gamma_g \times \Gamma_g$ such that

$$|\mathbf{cor}_{E_k}(\gamma,\gamma')| \geq \frac{1}{|\Gamma_g|}$$

directly follows. The fact that γ and γ' differ from zero is guaranteed by the fact that g is balanced, i.e., $0 \notin \Gamma_g$. □

3.1.2 Examples

In Midori64, the block size is $n = 64$ and, if we denote the bits in the j-th cell of the state by $x_{j,3}, x_{j,2}, x_{j,1}, x_{j,0}$ (where the lsb corresponds to $x_{j,0}$), the nonlinear invariant is given by

$$g(x) = \sum_{j=0}^{15} (x_{j,3}x_{j,2} + x_{j,2} + x_{j,1} + x_{j,0}) \ .$$

Equation (2) holds with $\Gamma_g = \{(\gamma_0, \ldots, \gamma_{15}) \mid \forall j : \gamma_{j,0} = \gamma_{j,1} = 1\}$ and

$$f(\gamma) = \sum_{j=0}^{15} \gamma_{j,3}\gamma_{j,2} + \gamma_{j,3} \ .$$

In SCREAM, the block size is $n = 128$ and the nonlinear invariant is given by

$$g(x) = \sum_{j=0}^{15} (x_{j,2}x_{j,1} + x_{j,5} + x_{j,2} + x_{j,0}) \ .$$

Equation (2) holds with

$$\Gamma_g = \{(\gamma_0, \ldots, \gamma_{15}) \mid \forall j : \gamma_{j,0} = \gamma_{j,5} = 1, \gamma_{j,3} = \gamma_{j,4} = \gamma_{j,6} = \gamma_{j,7} = 0\}$$

and

$$f(\gamma) = \sum_{j=0}^{15} \gamma_{j,2}\gamma_{j,1} + \gamma_{j,2} \ .$$

In iSCREAM, the block size is $n = 128$ and the nonlinear invariant is given by

$$g(x) = \sum_{j=0}^{15} (x_{j,5}x_{j,4} + x_{j,6} + x_{j,0}) \ .$$

Equation (2) holds with

$$\Gamma_g = \{(\gamma_0, \ldots, \gamma_{15}) \mid \forall j : \gamma_{j,0} = \gamma_{j,6} = 1, \gamma_{j,1} = \gamma_{j,2} = \gamma_{j,3} = \gamma_{j,7} = 0\}$$

and

$$f(\gamma) = \sum_{j=0}^{15} \gamma_{j,5}\gamma_{j,4} \ .$$

3.2 The Case of Invariant Subspaces

The case of invariant subspaces is not directly covered by Theorem 4 since the corresponding indicator function g is not balanced (unless the subspace has dimension $(n-1)$ which would mean that the cipher has a linear approximation holding with probability 1). However, we can prove a similar result: The existence of an invariant subspace implies the existence of a linear approximation of the cipher with a high bias. The result is even stronger than in the previous case since many such linear approximations can be exhibited.

Theorem 5. *Let $(U + a) \subseteq \mathbb{F}_2^n$ be an affine subspace of $\mathbb{F}_2^n$ invariant under E_k. Then, for any nonzero $\gamma' \in U^\perp$, there exists a $\gamma \in U^\perp \setminus \{0\}$ such that*

$$\mathbf{cor}_{E_k}(\gamma, \gamma') \geq 2^{-n+\dim U} \ ,$$

where $U^\perp$ denotes the orthogonal of U.

Proof. We first prove the following well-known result (e.g., [CC03, Prop. 1]) for the sake of clarity: For any $\gamma' \in U^\perp$, we have

$$\begin{aligned}
\sum_{\gamma \in U^\perp} (-1)^{\langle \gamma, a \rangle} \mathbf{cor}_{E_k}(\gamma, \gamma') &= 2^{-n} \sum_{\gamma \in U^\perp} (-1)^{\langle \gamma, a \rangle} \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle \gamma', E_k(x) \rangle + \langle \gamma, x \rangle} \\
&= 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle \gamma', E_k(x) \rangle} \left(\sum_{\gamma \in U^\perp} (-1)^{\langle \gamma, a+x \rangle} \right) \\
&= 2^{-\dim U} \sum_{x \in U+a} (-1)^{\langle \gamma', E_k(x) \rangle} \ ,
\end{aligned}$$

where the last equality comes from the fact that, for any linear space V,

$$\sum_{x\in V}(-1)^{\langle\alpha,x\rangle} = \begin{cases} 2^{\dim V} & \text{if } \alpha \in V^\perp \\ 0 & \text{otherwise} \end{cases}$$

that we apply here to $V = U^\perp$. Now, if $(U + a)$ is invariant under E_k, then $E_k(x)$ belongs to $(U + a)$ for all $x \in (U + a)$. This implies that $\langle\gamma', E_k(x)\rangle = \langle\gamma', a\rangle$ because $\gamma' \in U^\perp$. We then deduce that

$$\sum_{x\in U+a}(-1)^{\langle\gamma',E_k(x)\rangle} = (-1)^{\langle\gamma',a\rangle}2^{\dim U} ,$$

or equivalently

$$\left|\sum_{\gamma\in U^\perp}(-1)^{\langle\gamma,a\rangle}\,\mathbf{cor}_{E_k}(\gamma,\gamma')\right| = 1 . \tag{3}$$

It follows that, for any nonzero $\gamma' \in U^\perp$, there exists a γ such that

$$|\,\mathbf{cor}_{E_k}(\gamma,\gamma')| \geq 2^{-n+\dim U} .$$

Obviously, this γ differs from 0 since $\mathbf{cor}_{E_k}(0,\gamma') = 0$ if $\gamma' \neq 0$. □

Already in [LAAZ11], the authors deduced the existence of a highly-biased linear approximation from an invariant subspace. In particular, they showed the existence of a linear approximation with an absolute correlation greater than or equal to

$$2^{-n+\dim U} - 2^{2(-n+\dim U)} .$$

Thus, our result slightly improves this bound and further shows the existence of such a linear approximation *for all possible output masks in* $U^\perp$.

4 Probabilistic Nonlinear Approximations for Cryptanalysis

In this section, we explain how nonlinear invariants, and more generally probabilistic nonlinear approximations, can be studied in the framework of linear cryptanalysis.

4.1 Transforming Nonlinear Invariants into Linear Trails

Since linear approximations seem to be much easier to handle, we use the following trick which enables us to transform *a balanced nonlinear invariant* g into an *invariant hyperplane*. When g is *balanced*, one can embed g into a bijection $\mathcal{G} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for which $g(x) = \langle\alpha, \mathcal{G}(x)\rangle$ for some $\alpha \in \mathbb{F}_2^n$, i.e., g can be considered as one component function of $\mathcal{G}$. The fact that g is an invariant for E_k when k is weak means that there exists an $\varepsilon_k \in \mathbb{F}_2$ such that

$$\forall x : \langle\alpha, \mathcal{G}(x)\rangle = \langle\alpha, \mathcal{G}(E_k(x))\rangle + \varepsilon_k .$$

Since $\mathcal{G}$ is a bijection, this holds if and only if

$$\forall x : \langle\alpha, x\rangle = \langle\alpha, \mathcal{G}(E_k(\mathcal{G}^{-1}(x))\rangle + \varepsilon_k .$$

Thus, one can understand the invariant attack as having a transformed cipher $E_k^{\mathcal{G},\mathcal{G}^{-1}} := \mathcal{G} \circ E_k \circ \mathcal{G}^{-1}$ for which $E_k^{\mathcal{G},\mathcal{G}^{-1}}$ has a *linear approximation with absolute correlation 1*, i.e.,

$$\left|\mathbf{cor}_{E_k^{\mathcal{G},\mathcal{G}^{-1}}}(\alpha,\alpha)\right| = 1 .$$

In other words, replacing E_k by the transformed cipher $E_k^{\mathcal{G},\mathcal{G}^{-1}}$ boils down to replacing the invariant set $I := \{x \in \mathbb{F}_2^n : g(x) = 1\} \subset \mathbb{F}_2^n$, of size 2^{n-1}, by the affine hyperplane $H := \{y \in \mathbb{F}_2^n : \langle \alpha, y\rangle = 1\}$. Indeed, for any $y \in \mathcal{G}(I)$, there exists an $x \in \mathbb{F}_2^n$ such that

$$\langle \alpha, y\rangle = \langle \alpha, \mathcal{G}(x)\rangle = g(x) = 1 \; .$$

This implies that $\mathcal{G}(I) = H$. It follows that $\mathcal{G} \circ E_k \circ \mathcal{G}^{-1}(H) = H$, i.e., H is an invariant subspace for the transformed cipher $E_k^{\mathcal{G},\mathcal{G}^{-1}}$.

So far, we have considered the invariant attack as a linear approximation $\alpha \to \alpha$ over a transformed cipher $E_k^{\mathcal{G},\mathcal{G}^{-1}}$ that holds with absolute correlation 1. In a more general setting, the adversary can try to find a transformation $E_k^{\mathcal{G},\mathcal{G}^{-1}}$ and masks $\alpha, \beta \in \mathbb{F}_2^n$ such that, for each weak key k, the approximation $\alpha \to \beta$ holds with a *high* absolute correlation, not necessarily equal to 1. This leads to the utilization of *probabilistic nonlinear approximations*.

If $E_{(k_0,\ldots,k_t)}$ is a round-iterated cipher where $\mathcal{R}_{k_i}$ denotes the keyed round using the round key k_i, we have

$$E_{(k_0,\ldots,k_t)}^{\mathcal{G},\mathcal{G}^{-1}} = \mathcal{G} \circ \mathcal{R}_{k_t} \circ \mathcal{R}_{k_{t-1}} \circ \cdots \circ \mathcal{R}_{k_0} \circ \mathcal{G}^{-1} = \mathcal{R}_{k_t}^{\mathcal{G},\mathcal{G}^{-1}} \circ \mathcal{R}_{k_{t-1}}^{\mathcal{G},\mathcal{G}^{-1}} \circ \cdots \circ \mathcal{R}_{k_0}^{\mathcal{G},\mathcal{G}^{-1}} .$$

Using Theorem 1, the correlation of the approximation $\alpha \overset{E_k^{\mathcal{G},\mathcal{G}^{-1}}}{\to} \beta$ can be expressed as

$$\mathbf{cor}_{E_{(k_0,\ldots,k_t)}^{\mathcal{G},G^{-1}}}(\alpha,\beta) = \sum_{\gamma_1,\ldots,\gamma_{t-1} \in \mathbb{F}_2^n} \prod_{i=0}^{t-1} \mathbf{cor}_{\mathcal{R}_{k_i}^{\mathcal{G},\mathcal{G}^{-1}}}(\gamma_i, \gamma_{i+1}) \; , \tag{4}$$

where $\gamma_0 = \alpha, \gamma_t = \beta$ and $\gamma = (\gamma_0, \ldots, \gamma_t)$. Here, γ is similar to what is called a linear trail in Equation (1). The difference is that the γ_i are the intermediate masks shifted by the transformation $\mathcal{G}$. We therefore call γ a *$\mathcal{G}$-shifted linear trail* through E_k. Its correlation is defined as $\prod_{i=0}^{t-1} \mathbf{cor}_{\mathcal{R}_{k_i}^{\mathcal{G},\mathcal{G}^{-1}}}(\gamma_i, \gamma_{i+1})$.

Moreover, it is important to note that from Theorem 1, the correlation of the transformed cipher is given by

$$\begin{aligned} \mathbf{cor}_{E_k^{\mathcal{G},G^{-1}}}(\alpha,\beta) &= \sum_{\gamma_1,\gamma_2 \in \mathbb{F}_2^n} \mathbf{cor}_{\mathcal{G}^{-1}}(\alpha,\gamma_1)\, \mathbf{cor}_{E_k}(\gamma_1,\gamma_2)\, \mathbf{cor}_{\mathcal{G}}(\gamma_2,\beta) \\ &= \sum_{\gamma_1,\gamma_2 \in \mathbb{F}_2^n} \mathbf{cor}_{\mathcal{G}_\alpha}(\gamma_1)\, \mathbf{cor}_{E_k}(\gamma_1,\gamma_2)\, \mathbf{cor}_{\mathcal{G}_\beta}(\gamma_2) \end{aligned}$$

where $\mathcal{G}_\alpha$ (resp. $\mathcal{G}_\beta$) denotes the component function of $\mathcal{G}$: $x \mapsto \langle \alpha, \mathcal{G}(x)\rangle$ (resp. $x \mapsto \langle \beta, \mathcal{G}(x)\rangle$). Obviously, the correlation of the approximation

$$\alpha \overset{E_k^{\mathcal{G},\mathcal{G}^{-1}}}{\to} \beta$$

depends on these two components of $\mathcal{G}$ only. However, the correlation of a $\mathcal{G}$-shifted linear trail through E_k may depend on the other components of $\mathcal{G}$. This dependence then cancels out when summing the correlations of all trails corresponding to a given approximation.

For the sake of simplicity, we here concentrate on the case where the same transformation $\mathcal{G}$ is used all along the trail. However, a similar analysis holds by using the decomposition

$$E_{(k_0,\ldots,k_t)}^{\mathcal{G},\mathcal{G}^{-1}} = \mathcal{G} \circ \mathcal{R}_{k_t} \circ \mathcal{R}_{k_{t-1}} \circ \cdots \circ \mathcal{R}_{k_0} \circ \mathcal{G}^{-1} = \mathcal{R}_{k_t}^{\mathcal{G},\mathcal{G}_t^{-1}} \circ \mathcal{R}_{k_{t-1}}^{\mathcal{G}_t,\mathcal{G}_{t-1}^{-1}} \circ \cdots \circ \mathcal{R}_{k_0}^{\mathcal{G}_1,\mathcal{G}^{-1}},$$

for any choice of the permutations $\mathcal{G}_1, \ldots, \mathcal{G}_t$. Again, the correlation of the approximation

$$\alpha \overset{E_k^{\mathcal{G},\mathcal{G}^{-1}}}{\to} \beta$$

does not depend on the choice of the intermediate permutations $\mathcal{G}_1, \ldots, \mathcal{G}_t$, but the correlation of each individual trail does.

4.2 The Nonlinear Invariant Attack on Midori64

We first describe the nonlinear invariant attack on Midori64 given in [TLS16] in terms of a $\mathcal{G}$-shifted linear trail (see Figure 1). The attack uses the 4-bit Boolean function $g(x) = x_3x_2 + x_2 + x_1 + x_0$ which is invariant for a single S-box S. Without loss of generality, let G be a bijection on 4 bits that embeds g as its first coordinate function, i.e., $g(x) = \langle 8, G(x)\rangle = G_8$. Then, $\mathcal{G} \coloneqq (G, G, \ldots, G)$ is defined as the parallel application of 16 copies of G.

The round function of Midori64 can be described as $\mathcal{R}_k = \mathcal{M} \circ \mathcal{P} \circ \mathcal{S}_k$, where $\mathcal{S}_k$ applies the round key addition with k followed by a 16-times parallel application of the 4-bit S-box S, $\mathcal{P}$ applies a word-wise permutation of the 4-bit words of the state (PermuteCells layer), and $\mathcal{M}$ denotes the MixColumns operation. We view the transformed round function as $\mathcal{R}_k^{\mathcal{G},\mathcal{G}^{-1}} = \mathcal{M}^{\mathcal{G},\mathcal{G}^{-1}} \circ \mathcal{P}^{\mathcal{G},\mathcal{G}^{-1}} \circ \mathcal{S}_k^{\mathcal{G},\mathcal{G}^{-1}}$.

The Key Addition and the S-box Layer

Since g is invariant for the S-box S and since g is linear in x_0, x_1, also g is invariant for S_k when $k \in \mathrm{WK} := \{(0, 0, y_1, y_0) \mid y_0, y_1 \in \mathbb{F}_2\}$. In our setting, this implies that $|\mathbf{cor}_{S_k^{G,G^{-1}}}(8, 8)| = 1$ for $k \in \mathrm{WK}$. Moreover, for all other keys, the correlation is equal to 0.

For the whole S-box layer $\mathcal{S} = (S, S, \ldots, S)$ and for general input and output masks $\alpha_i, \beta_i \in \mathbb{F}_2^4$, with $0 \le i < 16$, we have

$$\left|\mathbf{cor}_{\mathcal{S}_k^{\mathcal{G},\mathcal{G}^{-1}}}((\alpha_0, \ldots, \alpha_{15}), (\beta_0, \ldots, \beta_{15}))\right| = \prod_{j=0}^{15} \left|\mathbf{cor}_{S_{k_j}^{G,G^{-1}}}(\alpha_j, \beta_j)\right|.$$

In our case, it leads to

$$\left|\mathbf{cor}_{\mathcal{S}_k^{\mathcal{G},\mathcal{G}^{-1}}}((8, 8, \ldots, 8), (8, 8, \ldots, 8))\right| = \prod_{j=0}^{15} \left|\mathbf{cor}_{S_{k_j}^{G,G^{-1}}}(8, 8)\right|$$

which is equal to 1 if all $k_j \in \mathrm{WK}$ and 0 for all other keys k. Therefore, the set of weak round keys for the whole state is $\mathcal{WK} := \mathrm{WK}^{16}$.

The PermuteCells and MixColumns Layer

The PermuteCells layer $\mathcal{P}$ just permutes the nibbles of the state according to the Midori64 cell permutation π. Since each G operates independently on each of the cells, we have that $\mathcal{P}^{\mathcal{G},\mathcal{G}^{-1}} = \mathcal{P}$. Thus,

$$\mathbf{cor}_{\mathcal{P}^{\mathcal{G},\mathcal{G}^{-1}}}((\alpha_0, \ldots, \alpha_{15}), (\beta_0, \ldots, \beta_{15})) = \begin{cases} 1 & \text{if } \forall i : \alpha_i = \beta_{\pi(i)} \\ 0 & \text{otherwise} \end{cases}. \tag{5}$$

Since in our case, $\alpha_i = \beta_i = 8$ for all i, the linear approximation trivially holds with correlation 1.

The MixColumns layer $\mathcal{M}$ multiplies each column of the state by the 4×4 binary matrix

$$\mathbf{M} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

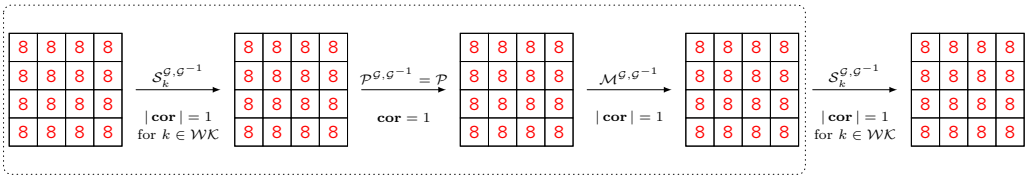

Figure 1: The $\mathcal{G}$-shifted linear trail for one round of Midori64 corresponding to the invariant attack. $\mathcal{G} = (G, G, \ldots, G)$ is any permutation for which $\langle \mathsf{8}, G(x)\rangle$ is equal to the invariant $g(x) = x_3x_2 + x_2 + x_1 + x_0$ for the S-box. In this trail, all S-boxes are active.

Let $\mathbf{G} \coloneqq (G, G, G, G)$. Now, the correlation can be computed as

$$\begin{aligned} & |\,\mathbf{cor}_{\mathcal{M}^{\mathcal{G},\mathcal{G}^{-1}}}\left((\alpha_0, \ldots, \alpha_{15}), (\beta_0, \ldots, \beta_{15})\right)| \\ = & \prod_{j=0}^{3} |\,\mathbf{cor}_{\mathbf{M}^{\mathbf{G},\mathbf{G}^{-1}}}\left((\alpha_{4j}, \alpha_{4j+1}, \alpha_{4j+2}, \alpha_{4j+3}), (\beta_{4j}, \beta_{4j+1}, \beta_{4j+2}, \beta_{4j+3})\right)| \,. \end{aligned}$$

Since G_{8} is a quadratic function and since $\mathbf{M}$ is a binary orthogonal matrix, from Theorem 1 in [TLS16], it follows that

$$|\,\mathbf{cor}_{\mathbf{M}^{\mathbf{G},\mathbf{G}^{-1}}}\left((\mathsf{8},\mathsf{8},\mathsf{8},\mathsf{8}), (\mathsf{8},\mathsf{8},\mathsf{8},\mathsf{8})\right)| = 1 \,.$$

This can also easily be verified by looking at the correlation matrix of $\mathbf{M}^{\mathbf{G},\mathbf{G}^{-1}}$.

All in all, this leads to a $\mathcal{G}$-shifted linear trail through an arbitrary number of rounds $\mathcal{R}_{k_i}^{\mathcal{G},\mathcal{G}^{-1}}$ of Midori64 that holds with absolute correlation equal to 1 if and only if all round keys k_i are in the set of weak keys $\mathcal{WK}$. In this trail, all S-boxes are active, i.e., all S-boxes get the non-zero input mask $\mathsf{8}$ (see Figure 1). It is important to note that, since the absolute correlation of this $\mathcal{G}$-shifted linear trail is equal to 1, the linear hull as given in Equation (4) contains no other $\mathcal{G}$-shifted linear trails that have a non-zero correlation.

The property of all round keys being in $\mathcal{WK}$ is fulfilled for a fraction of 2^{-64} of all the possible initial keys.

4.3 A Probabilistic Nonlinear Approximation for Four Rounds of Midori64

We give an example of a probabilistic nonlinear approximation on four rounds of Midori64 *with independent round keys*. This means we omit the key schedule and allow arbitrary keys in each round. Thus, for four rounds, there are 2^{256} possible keys. The idea is to find a permutation $\mathcal{G}'$ and to construct a $\mathcal{G}'$-shifted linear trail – similar to the one depicted in Figure 1 – that holds with a high (enough) absolute correlation. Note that – by design of Midori64 – the absolute correlation of any four-round linear trail can be upper bounded by 2^{-16} as there are at least 16 active S-boxes in four rounds and the maximum absolute correlation over the S-box is 2^{-1}. In comparison, the absolute correlation of our four-round $\mathcal{G}'$-shifted linear trail (as depicted in Figure 2) is only $2^{-12.325}$. The number of weak keys is 2^{208} out of all 2^{256} possible keys.

The $\mathcal{G}$-shifted trail corresponding to the nonlinear invariant attack has all S-boxes active. Here, we reduce the number of active S-boxes in order to allow a larger space of weak keys.

The Permutation $\mathcal{G}'$

The bijection $\mathcal{G}'$ we are using is the 16-time parallel application of the 4-bit permutation G' for which $\langle \mathsf{8}, G'(x)\rangle = g'(x) = x_3x_2x_1 + x_3x_1 + x_3 + x_2 + x_1 + x_0$.

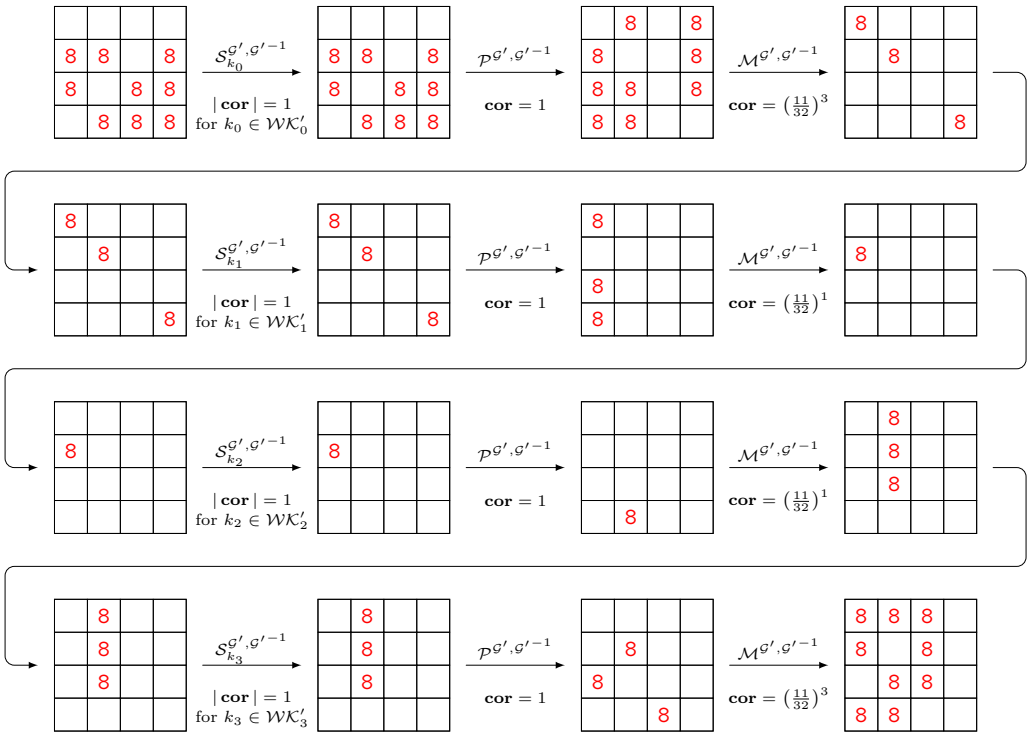

Figure 2: A probabilistic $\mathcal{G}'$-shifted linear trail for four rounds of Midori64.

Correlation over $\mathcal{S}_{\boldsymbol{k}}^{\mathcal{G}',\mathcal{G}'^{-1}}$

The permutation G' has the property that the absolute correlation of $8 \to 8$ over $S_k^{G',G'^{-1}}$ is equal to 1 for $k \in \mathrm{WK}' \coloneqq \{(0,0,0,0),(0,0,0,1)\}$.

Correlation over $\mathcal{P}^{\mathcal{G}',\mathcal{G}'^{-1}}$

Again, we have that $\mathcal{P}^{\mathcal{G}',\mathcal{G}'^{-1}} = \mathcal{P}$ and Equation (5) holds.

Correlation over $\mathcal{M}^{\mathcal{G}',\mathcal{G}'^{-1}}$

Let $\mathbf{G}' := (G', G', G', G')$. Now, by computing the LAT of $\mathbf{M}^{\mathbf{G}',\mathbf{G}'^{-1}}$, one obtains

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

if $\alpha \neq (0,0,0,0)$ and all $\alpha_i \in \{0, 8\}$. If the column is not active, i.e., if $\alpha = (0,0,0,0)$, the correlation is equal to 1.

Putting All Together

One can construct a four-round $\mathcal{G}'$-shifted linear trail that holds with an absolute correlation of $2^{-12.325}$ if all the round keys are weak (See Figure 2). Weak keys are those that are $(0,0,0,0)$ or $(0,0,0,1)$ in all active cells. The subkey in each of the inactive cells can be arbitrary.

It is worth remarking that the correlation of this $\mathcal{G}'$-shifted linear trail is independent of all component functions of G' except G'_8. However, opposed to the $\mathcal{G}$-shifted linear trail

given in Section 4.2, its absolute correlation is not equal to 1 and thus, the linear hull may contain other valid $\mathcal{G}'$-shifted linear trails. Which trails exactly and their corresponding correlations depend on the other components of G'. As an illustration, we computed the number of constituent $\mathcal{G}'$-shifted linear trails for the approximation corresponding to the first two rounds of the trail depicted in Figure 2. We used the following two 4-bit permutations G'_1 and G'_2 which both satisfy $\langle \mathtt{8}, G'_i(x)\rangle = g'(x)$:

$$G'_1 = [\mathtt{0},\mathtt{8},\mathtt{c},\mathtt{4},\mathtt{a},\mathtt{2},\mathtt{6},\mathtt{e},\mathtt{9},\mathtt{1},\mathtt{d},\mathtt{5},\mathtt{3},\mathtt{b},\mathtt{f},\mathtt{7}]$$
$$G'_2 = [\mathtt{0},\mathtt{9},\mathtt{a},\mathtt{1},\mathtt{8},\mathtt{2},\mathtt{3},\mathtt{f},\mathtt{c},\mathtt{4},\mathtt{d},\mathtt{5},\mathtt{6},\mathtt{e},\mathtt{b},\mathtt{7}]$$

It can be observed that, with the exception of $x \mapsto \langle \mathtt{8}, G'_1(x)\rangle$, the coordinates of G'_1 are linear, while the coordinates of G'_2 have degree 3. More precisely, $\langle \mathtt{1}, G'_1(x)\rangle = x_3$, $\langle \mathtt{2}, G'_1(x)\rangle = x_2$, $\langle \mathtt{4}, G'_1(x)\rangle = x_1$, and,

$$\begin{aligned}
\langle \mathtt{1}, G'_2(x)\rangle &= x_0x_2x_3 + x_1x_2x_3 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_0\ ,\\
\langle \mathtt{2}, G'_2(x)\rangle &= x_0x_1x_3 + x_0x_2x_3 + x_0x_1 + x_0x_2 + x_1x_3 + x_2x_3 + x_1\ ,\\
\langle \mathtt{4}, G'_2(x)\rangle &= x_0x_1x_2 + x_1x_2x_3 + x_3\ .
\end{aligned}$$

Then, the linear hull of this two-round approximation contains $35,937$ $\mathcal{G}'_1$-shifted linear trails having a nonzero correlation when G'_1 is used, and $282,184$ $\mathcal{G}'_2$-shifted linear trails having a nonzero correlation when G'_2 is used. Among those trails, the trail depicted in Figure 2 has the highest absolute correlation, i.e., $\left(\frac{11}{32}\right)^4 = 0.013963$. This value is close to the correlation of the approximation which equals 0.013062. Indeed, in both cases, the vast majority of trails have a very low correlation, typically with absolute value less than 2^{-16}. However, as already explained before, the resulting correlation of the nonlinear approximation only depends on $x \mapsto \langle \mathtt{8}, G'(x)\rangle = g'(x)$ and is independent of the other coordinates of the considered permutation G'.

In order to see whether the correlation of our given $\mathcal{G}'$-shifted linear trail can be used to approximate the correlation of the approximation over a larger number of rounds, we fixed one of the 2^{208} weak keys and experimentally computed the correlation. In particular, for three rounds (the first three rounds of the trail), we get an estimation for the absolute correlation of roughly $2^{-7.49}$ using 2^{28} randomly chosen plaintexts. Note that we expect a correlation of $(11/32)^5 = 2^{-7.703}$ from the $\mathcal{G}'$-shifted linear trail. For the four-round case, we get an estimate for the absolute correlation of $\approx 2^{-12.16}$ using 2^{32} randomly chosen plaintexts.

4.4 A Trail for Full-Round Midori64 and a Strong Linear Hull Effect

So far, we were able to express the approximation $\alpha \to \beta$ over a transformed round $\mathcal{R}_{k_i}^{\mathcal{G},\mathcal{G}^{-1}}$ as a single trail through the keyed S-box layer and the linear layer, i.e.,

$$\begin{aligned}
|\,\mathbf{cor}_{\mathcal{R}_{k_i}^{\mathcal{G},\mathcal{G}^{-1}}}(\alpha,\beta)| &= \left|\sum_{\gamma} \mathbf{cor}_{\mathcal{S}_{k_i}^{\mathcal{G},\mathcal{G}^{-1}}}(\alpha,\gamma)\,\mathbf{cor}_{\mathcal{L}^{\mathcal{G},\mathcal{G}^{-1}}}(\gamma,\beta)\right| \\
&= |\,\mathbf{cor}_{\mathcal{S}_{k_i}^{\mathcal{G},\mathcal{G}^{-1}}}(\alpha,\alpha)\,\mathbf{cor}_{\mathcal{L}^{\mathcal{G},\mathcal{G}^{-1}}}(\alpha,\beta)| = |\,\mathbf{cor}_{\mathcal{L}^{\mathcal{G},\mathcal{G}^{-1}}}(\alpha,\beta)|.
\end{aligned}$$

The reason for this is that we have chosen input masks α that propagate through $\mathcal{S}_k^{\mathcal{G},\mathcal{G}^{-1}}$ to the output mask α with absolute correlation 1. In principle, one can also consider masks (and keys) such that this propagation is not deterministic (the corresponding shifted trail will also consider intermediate masks after $\mathcal{S}_k^{\mathcal{G},\mathcal{G}^{-1}}$).

We can give an example of such a trail through the full-round version of Midori64 (also taking care of the actual key schedule!).

The Permutation $\mathcal{G}''$

The bijection $\mathcal{G}''$ is very similar to $\mathcal{G}$ above. The only difference is that the 4-bit sub-permutation G of the upper left cell of the state is replaced by G'. Thus, $\mathcal{G}'' = (G', G, G, \ldots, G)$.

Correlation over $\mathcal{S}_k^{\mathcal{G}'',\mathcal{G}''^{-1}}$

The permutation G' has the nice property that the correlation of $\mathtt{8} \to \mathtt{8}$ over $S_k^{G',G'^{-1}}$ is non-zero for all the keys $k \in \mathbb{F}_2^4$. In particular, it is

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

Since in all other cells of the state, the permutation G is the same as above, it is

$$\begin{aligned} &|\,\mathbf{cor}_{\mathcal{S}_{k_i}^{\mathcal{G}'',\mathcal{G}''^{-1}}}((\mathtt{8},\mathtt{8},\ldots,\mathtt{8}),(\mathtt{8},\mathtt{8},\ldots,\mathtt{8}))\,| \\ &= |\,\mathbf{cor}_{S_{k_{i,0}}^{G',G'^{-1}}}(\mathtt{8},\mathtt{8})| \prod_{j=1}^{15} |\,\mathbf{cor}_{S_{k_{i,j}}^{G,G^{-1}}}(\mathtt{8},\mathtt{8})| \geq 2^{-1} \end{aligned}$$

if the round key $k_i \in \mathcal{WK}'' := \mathbb{F}_2^4 \times \{(0,0,*,*)\}^{15}$.

Correlation over $\mathcal{P}^{\mathcal{G}',\mathcal{G}'^{-1}}$

The PermuteCells layer $\mathcal{P}$ does not permute the upper-left cell of the state. Therefore, we again have $\mathcal{P}^{\mathcal{G}'',\mathcal{G}''^{-1}} = \mathcal{P}$ and $(\mathtt{8},\ldots,\mathtt{8}) \to (\mathtt{8},\ldots,\mathtt{8})$ holds with correlation 1.

Correlation over $\mathcal{M}^{\mathcal{G}'',\mathcal{G}''^{-1}}$

Let again $\mathbf{G} := (G,G,G,G)$ and let further $\mathbf{G}'' := (G',G,G,G)$. Now, one obtains

$$\begin{aligned} &|\,\mathbf{cor}_{\mathcal{M}^{\mathcal{G}'',\mathcal{G}''^{-1}}}((\mathtt{8},\ldots,\mathtt{8}),(\mathtt{8},\ldots,\mathtt{8}))\,| \\ &= |\,\mathbf{cor}_{\mathbf{M}^{\mathbf{G}'',\mathbf{G}''^{-1}}}((\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8}),(\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8}))\,| \prod_{j=1}^{3} |\,\mathbf{cor}_{\mathbf{M}^{\mathbf{G},\mathbf{G}^{-1}}}((\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8}),(\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8}))\,| \\ &= |\,\mathbf{cor}_{\mathbf{M}^{\mathbf{G}'',\mathbf{G}''^{-1}}}((\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8}),(\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8}))\,| \approx 2^{-0.83} \end{aligned}$$

by computing the LAT of $\mathbf{M}^{\mathbf{G}'',\mathbf{G}''^{-1}}$.

Putting All Together

One finally obtains a shifted trail that holds with absolute correlation $\geq 2^{-1.83}$ over a single round of Midori64 if the round key belongs to the set of weak keys $\mathcal{WK}''$ (See Figure 3). Thus, for 16 rounds of Midori64, the absolute correlation can be lower bounded by $2^{-16\cdot 1.83} = 2^{-29.28}$. Based on this single trail, we should have a full-round distinguisher for Midori64 that works for a fraction of 2^{-60} of all the initial keys.

A Strong Linear-Hull Effect

It turns out that iterating the $\mathcal{G}''$-shifted linear trail given in Figure 3 over multiple rounds does not well approximate the linear hull and therefore, we do *not* have a full-round distinguisher as it was expected by the trail.

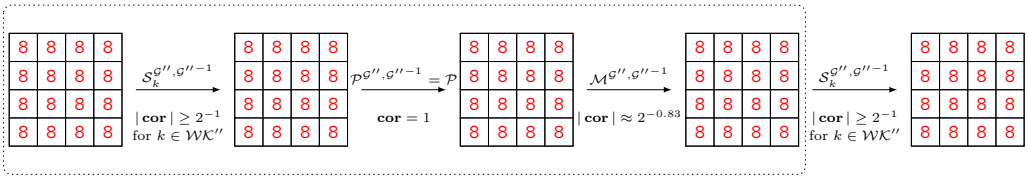

Figure 3: A $\mathcal{G}''$-shifted linear trail for the Midori64 round that considers the intermediate masks after $\mathcal{S}_k^{\mathcal{G}'',\mathcal{G}''^{-1}}$.

We can observe the linear-hull effect in more detail on a small-scale variant of Midori, which we define as two rounds operating on a single column. In particular, we consider the cipher defined by $E_{(k_0,k_1)} = \mathbf{M} \circ \mathbf{S}_{k_1} \circ \mathbf{M} \circ \mathbf{S}_{k_0}$, where $\mathbf{S} := (S, S, S, S)$ is the four-time parallel application of the Midori S-box, $\mathbf{M}$ the MixColumns matrix, and $k_0, k_1 \in \mathbb{F}_2^{16}$ the two round keys. For all $k_0, k_1 \in \mathbf{WK}'' := \mathbb{F}_2^4 \times \{(0,0,*,*)\}^3$, we computed the correlation of the approximation $(\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8}) \to (\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8})$ over $E_{(k_0,k_1)}^{\mathbf{G}'',\mathbf{G}''^{-1}}$. Our results are as follows: We obtain a correlation of exactly 0 if and only if $k_1 \in \left(\mathbb{F}_2^4 \setminus \{(0,0,*,*)\}\right) \times \{(0,0,*,*)\}^3$. In all other cases, the absolute correlation can take various values. In particular, if $k_0, k_1 \in \{(0,0,*,*)\}^4$, the set of possible values for the absolute correlation is

$$\{0.546875, 0.55859375, 0.5703125, 0.625\}\ .$$

If $k_0 \in \mathbb{F}_2^4 \setminus \{(0,0,*,*)\} \times \{(0,0,*,*)\}^3$ and $k_1 \in \{(0,0,*,*)\}^4$, the set of possible values for the absolute correlation is

$$\{0.15234375, 0.1640625, 0.16796875, 0.1796875, 0.19140625,\\ 0.203125, 0.21875, 0.23046875, 0.2421875, 0.25390625\}\ .$$

As examples, for fixed choices of k_1, we give the condition on k_0 that lead to the same value for the absolute correlation of the approximation in Tables 1, 2, 3, and 4, respectively.

Table 1: Fixing the second round key $k_1 = (\mathtt{0},\mathtt{0},\mathtt{0},\mathtt{0})$, this table shows all possible values for the absolute correlation of the approximation $(\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8}) \to (\mathtt{8},\mathtt{8},\mathtt{8},\mathtt{8})$ over $E_{(k_0,k_1)}^{\mathbf{G}'',\mathbf{G}''^{-1}}$ for k_0 from the set of weak keys $\mathbf{WK}''$.

abs. correlation	condition on k_0
0.625	$k_0 \in \{\mathtt{0},\mathtt{1}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\}$
0.5703125	$k_0 \in \{\mathtt{2},\mathtt{3}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\}$
0.2421875	$k_0 \in \{\mathtt{4},\mathtt{5},\mathtt{8},\mathtt{9},\mathtt{c},\mathtt{d},\mathtt{e},\mathtt{f}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\}$
0.25390625	$k_0 \in \{\mathtt{6},\mathtt{7},\mathtt{a},\mathtt{b}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\} \times \{\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3}\}$

5 Conclusion

In this work, we have studied a link between nonlinear and linear approximations in cryptanalysis. In the first part, i.e., Section 3, we have shown that in many practical cases a nonlinear invariant or an invariant subspace implies the existence of a highly-biased linear approximation. More precisely, we have improved the bound on the bias given in [LAAZ11] for the case of invariant subspaces, and we have exhibited a nonlinear counterpart by proving that the same result holds for many nonlinear invariants.

Table 2: Fixing the second round key $k_1 = (0, 0, 0, 1)$, this table shows all possible values for the absolute correlation of the approximation $(8, 8, 8, 8) \to (8, 8, 8, 8)$ over $E_{(k_0,k_1)}^{\mathbf{G}'',\mathbf{G}''^{-1}}$ for k_0 from the set of weak keys $\mathbf{WK}''$.

abs. correlation	condition on k_0
0.625	$k_0 \in \{0, 1\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.55859375	$k_0 \in \{2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.25390625	$k_0 \in \{4, 5\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.2421875	$k_0 \in \{6, 7, 8, 9\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.23046875	$k_0 \in \{a, b, c, d\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.21875	$k_0 \in \{e, f\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$

Table 3: Fixing the second round key $k_1 = (0, 0, 0, 2)$, this table shows all possible values for the absolute correlation of the approximation $(8, 8, 8, 8) \to (8, 8, 8, 8)$ over $E_{(k_0,k_1)}^{\mathbf{G}'',\mathbf{G}''^{-1}}$ for k_0 from the set of weak keys $\mathbf{WK}''$.

abs. correlation	condition on k_0
0.546875	$k_0 \in \{0, 1\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.55859375	$k_0 \in \{2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.15234375	$k_0 \in \{4, 5, 8, 9\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.1640625	$k_0 \in \{6, 7, c, d\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.19140625	$k_0 \in \{a, b\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.203125	$k_0 \in \{e, f\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$

Table 4: Fixing the second round key $k_1 = (0, 0, 0, 3)$, this table shows all possible values for the absolute correlation of the approximation $(8, 8, 8, 8) \to (8, 8, 8, 8)$ over $E_{(k_0,k_1)}^{\mathbf{G}'',\mathbf{G}''^{-1}}$ for k_0 from the set of weak keys $\mathbf{WK}''$.

abs. correlation	condition on k_0
0.546875	$k_0 \in \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.1640625	$k_0 \in \{4, 5\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.15234375	$k_0 \in \{6, 7, 8, 9, c, d\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.16796875	$k_0 \in \{a, b\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$
0.1796875	$k_0 \in \{e, f\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$

In the second part, i.e., Section 4, we have proposed a way to study nonlinear approximations in the framework of linear cryptanalysis by transforming the original cipher under consideration and applying linear cryptanalysis to the transformed cipher. We have seen an example in which an appropriate transformation reveals a weakness with regard to linear cryptanalysis that was claimed by the designers to be nonexistent based on the minimum number of active S-boxes.

Open Problems

One open issue raised in Section 3 would be to further characterize the highly-biased linear approximations that are implied by the invariants. For instance, if g denotes the invariant under consideration and k denotes a weak key, it would be nice to deduce something about the distribution of the values for $\mathbf{cor}_{E_k}(\gamma, \gamma')$ over all $\gamma, \gamma' \in \Gamma_g$. Actually, this is depending on the particular choice of k and, for an iterated cipher E, also on the number

of rounds.

A major open problem discussed in Section 4 is to understand the linear-hull effect with regard to the $\mathcal{G}$-shifted linear trails, and in particular the key dependency within those linear hulls. What is the particular reason that allows to approximate the correlation of the linear approximation by the shifted linear trail given in Figure 2 and what exactly goes wrong when utilizing the $\mathcal{G}''$-shifted trail given in Figure 3? In this context, a good start would be to further understand the linear-hull effect on the two-round small-scale variant of Midori described at the end of Section 4. In particular, the occurrence of the zero correlation is interesting here. For studying this linear-hull effect, we think that analyzing the other valid shifted linear trails is not very helpful as those (and their correlations) are depending on other components of the transformation $\mathcal{G}$. However, one can ask whether there exist some appropriate choices for the other components of $\mathcal{G}$ which make the analysis easier.

Another interesting question is whether we can use the presented framework on nonlinear approximations to describe clustering of linear approximations more generally and to establish to which kind of round functions exactly we can apply the framework.

As we have only given an example in which a transformed version of a cipher has a weaker resistance against linear cryptanalysis than the original one, future work would be to spot such kind of weaknesses in more existing ciphers.

Acknowledgements

We thank the anonymous reviewers for their helpful comments.

References

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 411–436. Springer, Heidelberg, 2015.

[BCLR17] Christof Beierle, Anne Canteaut, Gregor Leander, and Yann Rotella. Proving resistance against invariant attacks: How to choose the round constants. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 647–678. Springer, Heidelberg, August 2017.

[BDH+17] Guido Bertoni, Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. Farfalle: parallel permutation-based cryptography. *IACR Trans. Symmetric Cryptol.*, 2017(4):1–38, 2017.

[Bei18] Christof Beierle. *Design and analysis of lightweight block ciphers: a focus on the linear layer.* Doctoral thesis, Ruhr-Universität Bochum, Universitätsbibliothek, 2018.

[Bey18] Tim Beyne. Block cipher invariants as eigenvectors of correlation matrices. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 3–31. Springer International Publishing, 2018.

[Car07] Claude Carlet. Boolean Functions for Cryptography and Error Correcting Codes. In Yves Crama and Peter Hammer, editors, *Boolean Methods and Models*. Cambridge University Press, 2007.

[CC03] Anne Canteaut and Pascale Charpin. Decomposing bent functions. *IEEE Trans. Information Theory*, 49(8):2004–2019, 2003.

[CFG+17] Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jérémy Jean, and Jean-René Reinhard. Cryptanalysis of NORX v2.0. *IACR Trans. Symmetric Cryptol.*, 2017(1):156–174, 2017.

[DGV95] Joan Daemen, René Govaerts, and Joos Vandewalle. Correlation matrices. In Bart Preneel, editor, *FSE'94*, volume 1008 of *LNCS*, pages 275–285. Springer, Heidelberg, December 1995.

[DR07] Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *Journal of Mathematical Cryptology JMC*, 1(3):221–242, 2007.

[GJN+16] Jian Guo, Jérémy Jean, Ivica Nikolic, Kexin Qiao, Yu Sasaki, and Siang Meng Sim. Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs. *IACR Trans. Symmetric Cryptol.*, 2016(1):33–56, 2016.

[GLS+14] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici, Anthony Journault, François Durvaux, Lubos Gaspar, and Stéphanie Kerckhof. SCREAM v1, 2014. Submission to CAESAR.

[GLS+15] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici, Anthony Journault, François Durvaux, Lubos Gaspar, and Stéphanie Kerckhof. SCREAM v3, 2015. Submission to CAESAR.

[Har96] Carlo Harpes. *Cryptanalysis of iterated block ciphers.* PhD thesis, ETH Zurich, 1996.

[HKM95] Carlo Harpes, Gerhard G. Kramer, and James L. Massey. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *EUROCRYPT'95*, volume 921 of *LNCS*, pages 24–38. Springer, Heidelberg, May 1995.

[HM97] Carlo Harpes and James L. Massey. Partitioning cryptanalysis. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 13–27. Springer, Heidelberg, January 1997.

[Jea16] Jérémy Jean. Cryptanalysis of Haraka. *IACR Trans. Symmetric Cryptol.*, 2016(1):1–12, 2016.

[KR96] Lars R. Knudsen and Matthew J. B. Robshaw. Non-linear approximations in linear cryptoanalysis. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 224–236. Springer, Heidelberg, May 1996.

[LAAZ11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A cryptanalysis of PRINTcipher: The invariant subspace attack. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 206–221. Springer, Heidelberg, 2011.

[LMR15] Gregor Leander, Brice Minaud, and Sondre Rønjom. A generic approach to invariant subspace attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 254–283. Springer, Heidelberg, 2015.

[Mat94a] Mitsuru Matsui. The first experimental cryptanalysis of the data encryption standard. In Yvo Desmedt, editor, *CRYPTO'94*, volume 839 of *LNCS*, pages 1–11. Springer, Heidelberg, August 1994.

[Mat94b] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 386–397. Springer, Heidelberg, May 1994.

[Nyb95a] Kaisa Nyberg. Linear approximation of block ciphers. In Alfredo De Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 439–444. Springer, Heidelberg, May 1995.

[Nyb95b] Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In Bart Preneel, editor, *FSE'94*, volume 1008 of *LNCS*, pages 111–130. Springer, Heidelberg, December 1995.

[Pat99] Kenneth G. Paterson. Imprimitive permutation groups and trapdoors in iterated block ciphers. In Lars R. Knudsen, editor, *FSE'99*, volume 1636 of *LNCS*, pages 201–214. Springer, Heidelberg, March 1999.

[Røn16] Sondre Rønjom. Invariant subspaces in Simpira. Cryptology ePrint Archive, Report 2016/248, 2016. http://eprint.iacr.org/2016/248.

[TLS16] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear invariant attack - practical attack on full SCREAM, iSCREAM, and Midori64. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 3–33. Springer, Heidelberg, 2016.

[ZZ99] Yuliang Zheng and Xian-Mo Zhang. Plateaued functions. In Vijay Varadharajan and Yi Mu, editors, *ICICS 99*, volume 1726 of *LNCS*, pages 284–300. Springer, Heidelberg, November 1999.