Zero-Correlation Linear Cryptanalysis of Block Ciphers

Andrey Bogdanov and Vincent Rijmen

Katholieke Universiteit Leuven, ESAT/COSIC and IBBT, Belgium
{andrey.bogdanov, vincent.rijmen}@esat.kuleuven.be

Abstract. Linear cryptanalysis, along with differential cryptanalysis, is an important tool to evaluate the security of block ciphers. This work introduces a novel extension of linear cryptanalysis – *zero-correlation linear cryptanalysis* – a technique applicable to many block cipher constructions. It is based on linear approximations with a correlation value of exactly zero. For a permutation on n bits, an algorithm of complexity 2^{n-1} is proposed for the exact evaluation of correlation. Non-trivial zero-correlation linear approximations are demonstrated for various block cipher structures including AES, balanced Feistel networks, Skipjack, CLEFIA, and CAST256. Using the zero-correlation linear cryptanalysis, a key-recovery attack is shown on 6 rounds of AES-192 and AES-256 as well as 13 rounds of CLEFIA-256.
Keywords: block cipher, linear cryptanalysis, linear approximation, linear hull, correlation, evaluation of correlation, substitution-permutation network, Feistel cipher, AES, CLEFIA

1 Introduction

Block ciphers have evolved to be the basic primitives of symmetric-key cryptography. Many sound and efficient cryptographic constructions can be built upon them, such as stream ciphers, message authentication codes, hash functions or entropy extractors for random number generators. This is not least due to the fact that block ciphers possess a far developed analysis toolbox including the two major techniques — linear and differential cryptanalysis [5, 19]. Block ciphers are widely believed to be the best understood primitives of symmetric cryptography at hand. Nevertheless, also their security currently cannot be formally proven. Instead, we rely on cryptanalysis: careful evaluation against all the known weaknesses. Any significant advance in cryptanalytic techniques for block ciphers is of high relevance and might result in the re-evaluation of many designs. In this article, we propose a novel extension of linear cryptanalysis.

1.1 Motivation

Design strategies such as the wide trail design strategy [8] and the decorrelation theory [27] allow to construct block ciphers for which we can state with high confidence that they will resist crucial analysis methods such as differential cryptanalysis and linear cryptanalysis. However, these strategies provide only limited evidence of resistance against some extensions of differential cryptanalysis. While the original differential cryptanalysis exploits differentials holding with a relatively high probability, *impossible differential cryptanalysis* makes use of impossible differentials which are differentials

having a very low or even a zero probability [2,6]. Cryptanalysts have recently been quite active applying impossible differential cryptanalysis to various ciphers [3, 10, 16, 17, 26].

Similarly to differential cryptanalysis, the original linear cryptanalysis is based on linear approximations with correlations significantly deviating from zero. However, unlike differential cryptanalysis, for linear cryptanalysis there is only very limited work using linear approximations with correlation values of exactly zero [11].

In this work, we attempt to bridge this gap by enriching the cryptanalytic toolbox for block ciphers with a novel approach to linear cryptanalysis: *zero-correlation linear cryptanalysis* makes use of linear hulls with no linear trails, thus, having correlation zero. It can be considered as the counterpart of impossible differential cryptanalysis in the domain of linear cryptanalysis, though having many significant distinctions of both theoretical and technical nature. We apply it to balanced Feistel and generalized Feistel ciphers as well as to round-reduced AES.

1.2 Background

Idealized block cipher A block cipher operating on n-bit blocks with a k-bit key can be seen as a subset of cardinality 2^k of the set of all $2^n!$ permutations over the space of n-bit strings. In this paper, we are concerned with efficiently implementable block ciphers, for which a compact description exists and is public. Moreover, the key length k of efficient block ciphers is usually much smaller than $\log_2(2^n!)$, which implies that the block cipher realizes only a small subset of the n-bit permutations. We define a reference point for our attacks:

Definition 1 (Idealized block cipher). *An* idealized block cipher *with n-bit blocks and a k-bit key is a set of 2^k randomly drawn permutations on n-bit strings. The choice is performed randomly and uniformly from all $2^n!$ permutations on n bits.*

Furthermore, we are interested only in distinguishers of complexity smaller than 2^k.

Linear cryptanalysis and correlation Denote the scalar product of binary vectors by

$$a \diamond x = \bigoplus_{i=1}^{n} a_i x_i.$$

Linear cryptanalysis [19] uses *linear approximations* to build a distinguisher. A linear approximation $\alpha \rightarrow \beta$ of a binary transformation f is determined by the input and output selection patterns, α and β. The probability

$$p = \Pr_x\{\alpha \diamond x = \beta \diamond f(x)\}$$

computed over all inputs x can be used as a measure of approximation goodness. The more p deviates from $1/2$, the better the linear approximation is for linear cryptanalysis. Following [8] and [22], to characterize the deviation of p from $1/2$, we will operate here in terms of *correlation* C, which is related to p by: $C = 2p - 1$.

The correlation of linear approximation $0 \rightarrow 0$ is always 1. The correlation of linear approximation $\alpha \rightarrow 0$ is exactly zero for $\alpha \neq 0$. Furthermore, if f is a permutation, the

correlation of $0 \to \beta$ is also exactly zero for $\beta \neq 0$. We call such linear approximations *trivial* and the ones with both $\alpha \neq 0$ and $\beta \neq 0$ *non-trivial*.

For a randomly drawn n-bit permutation, the correlation C of a non-trivial linear approximation can be described as a stochastic variable with the following distribution [23, Theorem 1] and [9, Lemma 8]:

$$\Pr_f\left\{C = w \cdot 2^{2-n}\right\} = \frac{\binom{2^{n-1}}{2^{n-2}+w}^2}{\binom{2^n}{2^{n-1}}}. \tag{1}$$

Linear trails and linear hulls To make implementations compact and efficient, designers of block ciphers mostly opt for iterative transformations consisting of a number of (often similar) simpler maps, called *rounds*, applied iteratively.

A linear approximation $\alpha \to \beta$ of an iterative block cipher (or any other iterative transformation) is called a *linear hull* in [22]. The linear hull contains all possible sequences of the linear approximations for consecutive intermediate maps with input selection pattern α and output selection pattern β. These sequences are called *linear trails*.

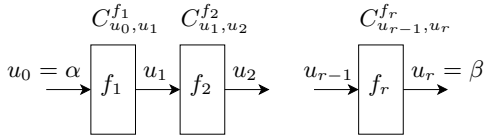

Fig. 1. Iterative transform $f : f_r \circ \cdots \circ f_1$ and a linear trail $U = (u_0, \ldots, u_r)$ of its linear hull $\alpha \to \beta$

More formally, let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an iterative transformation on n bits, that is, an iterative application of r maps f_i (rounds):

$$f = f_r \circ f_{r-1} \circ \ldots f_2 \circ f_1$$

with $f_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for each $i = 1, \ldots, r$. Consider a linear approximation $u_{i-1} \to u_i$ of a round map f_i with input selection pattern u_{i-1} and output selection pattern u_i. The linear approximation $u_{i-1} \to u_i$ over one round f_i is characterized by its correlation

$$C^{f_i}_{u_{i-1},u_i} = 2 \Pr_x\{u_{i-1} \diamond x = u_i \diamond f_i(x)\} - 1$$

computed over all round inputs x, see Figure 1.

Given a linear hull $\alpha \to \beta$ of the entire transformation f, a linear trail U is the concatenation of an input selection pattern $\alpha = u_0$ before f_0, an output selection pattern $\beta = u_r$ after f_r, and $r-1$ intermediate selection patterns u_i between the rounds f_{i-1} and f_i:

$$U = (u_0, u_1, \ldots, u_{r-1}, u_r).$$

Thus, each linear trail of f consists of $n(r+1)$ bits.

The *correlation contribution* C_U of linear trail U is defined as

$$C_U = \prod_{i=1}^{r} C_{u_{i-1},u_i}^{f_i}. \tag{2}$$

The theorem of linear trail composition [8, Theorem 7.8.1] states that for a linear hull $\alpha \to \beta$ of an iterative transformation f, its correlation C can be computed as the sum of correlation contributions C_U of all its linear trails U:

$$C = \sum_{U:u_0=\alpha,u_r=\beta} C_U \tag{3}$$

with input selection pattern α and output selection pattern β.

1.3 Contributions and outline

We propose a novel extension of linear cryptanalysis – zero-correlation linear attacks applicable to many block cipher constructions. We now discuss this in some more detail.

Zero-correlation linear hulls in block ciphers A *zero-correlation linear hull* can be seen as the counterpart in linear cryptanalysis of an impossible differential in differential cryptanalysis. It is a linear approximation over a block cipher having a correlation of exactly zero $C = 0$ which we denote by $\alpha \nrightarrow \beta$. To construct a zero-correlation linear hull in block ciphers, we choose the input and output selection patterns α and β such that there is no linear trail U with nonzero correlation contribution C_U to the linear hull correlation C.

In Section 3, using this result, we prove a sufficient condition for linear hulls of iterative ciphers to have zero correlation (Proposition 3). We also prove zero-correlation linear hulls over a number of rounds of AES [13] as well as several Feistel-type designs (balanced Feistel [12], Skipjack [25], CLEFIA [24], and CAST-256 [21]) illustrated in Figure 2. These findings are stated as Theorems 1 and 2. Table 1 compares the linear hulls that we found to the impossible differentials known in the literature.

Distinguishing with zero correlation In Section 2, we prove that for an idealized block cipher of sufficiently large block size n with a fixed key, the probability for a given non-trivial linear approximation to have a correlation of 0 is $\frac{1}{\sqrt{2\pi}} 2^{\frac{4-n}{2}}$ (Proposition 2). At the same time, the linear hulls of Table 1 have a zero correlation with probability 1 for any key value. This discrepancy provides a distinguisher with a low error probability.

The distinguisher relies on the precise evaluation of the correlation value for a given linear approximation. For an n-bit permutation, we show in Proposition 1 how to reduce the data complexity of the exact correlation evaluation down to 2^{n-1} by using chosen inputs or outputs. Algorithm 1 summarizes the procedure of the zero-correlation distinguisher.

Zero-correlation attack In Section 4, based on the zero-correlation linear hulls identified for AES and CLEFIA constructions as well as on the distinguisher of Algorithm 1, we propose a *key-recovery attack* on 6 rounds of AES-192 and 13 rounds of CLEFIA-256. The attack is somewhat similar to the impossible differential attack, but there are some important particularities, which follow from the difference between the mechanisms used in linear cryptanalysis and those in differential cryptanalysis. In particular distinguishing between a small correlation and a correlation that is exactly zero turns out to be difficult. Interestingly, this corresponds to the situation for ordinary linear and differential attacks: linear attacks usually can break a slightly smaller number of rounds than differential attacks (with a notable exception of DES where linear cryptanalysis tends to be more efficient [14, 15]).

Zero-correlation linear hulls are called *unbiased approximations* in [11] by Etrog and Robshaw. Although they also propose a linear attack, it is quite different from ours. Their zero-correlation linear hulls are created as follows: starting from an ordinary linear hull $\alpha \rightarrow \beta$ with correlation C, they derive the two linear hulls $\alpha \nrightarrow 0$ and $0 \nrightarrow \beta$, which have correlation zero for any invertible map. Subsequently, they show how to combine empirical measurements of the correlations of $\alpha \nrightarrow 0$ and $0 \nrightarrow \beta$ in order to obtain information on C. They observe that their attack is usually inferior to the classical linear attack using $\alpha \rightarrow \beta$. As opposed to [11], we use the zero-correlation linear hulls which are due to the specific high-level structure of ciphers to mount our attack. We conclude in Section 5.

2 Distinguisher of Zero Correlation

In this section, we propose a distinguisher for block ciphers with zero-correlation linear hulls. Moreover, we show how to evaluate the exact correlation value of a linear approximation more efficiently and derive the probability of zero correlation for an idealized block cipher.

2.1 Complexity reduction for correlation evaluation

Our extension of linear cryptanalysis for block ciphers is based on the exact evaluation of the correlation value for a linear approximation of a permutation. Let x and $y = f(x)$ be input and output of a permutation f. The straightforward way to evaluate the correlation is to use its definition by going over all 2^n input-output pairs and computing

$$C = 2p - 1 = \frac{|\{(x, y)|\alpha \diamond x \oplus \beta \diamond y = 0\}|}{2^{n-1}} - 1.$$

However, it is not necessary to have all 2^n input-output pairs to compute C:

Proposition 1 (Efficient correlation evaluation). *For any non-trivial linear approximation $\alpha \rightarrow \beta$ of a n-bit permutation f, the correlation value C can be evaluated with 2^{n-1} input-output pairs (x, y) in one of the following ways:*

$$\begin{aligned} C &= \frac{|\{(x, y)|\alpha \diamond x = 0 \text{ and } \beta \diamond y = 0\}|}{2^{n-2}} - 1 \\ &= \frac{|\{(x, y)|\alpha \diamond x = 1 \text{ and } \beta \diamond y = 1\}|}{2^{n-2}} - 1. \end{aligned}$$

Proof. The 2^n input-output pairs of an n-bit permutation can be divided into the following four disjunct sets:

$$\begin{aligned} T_{00} &= \{(x,y) | \alpha \diamond x = 0 \text{ and } \beta \diamond y = 0\}, \\ T_{01} &= \{(x,y) | \alpha \diamond x = 0 \text{ and } \beta \diamond y = 1\}, \\ T_{10} &= \{(x,y) | \alpha \diamond x = 1 \text{ and } \beta \diamond y = 0\}, \text{ and} \\ T_{11} &= \{(x,y) | \alpha \diamond x = 1 \text{ and } \beta \diamond y = 1\}. \end{aligned}$$

Since for a non-trivial linear approximation exactly one half of the inputs x yields $\alpha \diamond x = 0$ and the other half gives $\alpha \diamond x = 1$, one has:

$$|T_{00}| + |T_{01}| = 2^{n-1} \tag{4}$$

and

$$|T_{10}| + |T_{11}| = 2^{n-1}. \tag{5}$$

Moreover, this also applies to the outputs y of the permutation, since it is invertible:

$$|T_{01}| + |T_{11}| = 2^{n-1}. \tag{6}$$

Now subtracting (5) from (6), one gets

$$|T_{01}| = |T_{10}| \tag{7}$$

and subtracting (4) from (5) using (7) delivers

$$|T_{00}| = |T_{11}|. \tag{8}$$

Then by the definition of correlation, we obtain from (8):

$$C = 2p - 1 = 2\frac{|T_{00}| + |T_{11}|}{2^n} - 1 = \frac{|T_{00}|}{2^{n-2}} - 1 = \frac{|T_{11}|}{2^{n-2}} - 1.$$

Recalling the definitions of T_{00} and T_{11}, one obtains the claim of the proposition.

Proposition 1 says that for an n-bit permutation (e.g. a block cipher under a fixed key) it is possible to compute the exact value of C having only 2^{n-1} chosen input-output pairs (x, y) with one the the following four properties: either $\alpha \diamond x = 0$, $\alpha \diamond x = 1$, $\beta \diamond y = 0$, or $\beta \diamond y = 1$.

2.2 Probability of zero correlation

For a randomly drawn permutation on n bits, the correlation value for each non-trivial linear approximation will be as stated above in (1). Here we derive a compact and precise approximation of the probability that the correlation value is 0 for an idealized block cipher.

Proposition 2 (Zero correlation for idealized cipher). *The probability that the correlation value is 0 for a non-trivial linear approximation of an n-bit idealized cipher with a fixed key can be approximated by $\frac{1}{\sqrt{2\pi}} 2^{\frac{4-n}{2}}$ for $n \geq 5$.*

Proof. Recall Theorem 9 of [9]. It states that for a non-trivial linear approximation of an n-bit idealized block cipher under a fixed key (i.e. of a randomly drawn permutation) with $n \geq 5$ the distribution of the correlation value will be as follows:

$$\Pr\{C = z \cdot 2^{2-n}\} \approx \frac{1}{\sqrt{2\pi}2^{\frac{n-4}{2}}} e^{-\frac{z^2}{2^{n-3}}} \tag{9}$$

for integer z between -2^{n-2} and 2^{n-2}. By substituting $z = 0$, one obtains the claim of the proposition.

2.3 Distinguishing algorithm

To distinguish a block cipher with a zero-correlation linear hull from an idealized cipher, the adversary collects 2^{n-1} chosen plaintext-ciphertext pairs obtained under some fixed user-supplied key κ. The choice of either ciphertexts or plaintexts is performed using relations from Proposition 1. For the zero-correlation linear hull $\alpha \nrightarrow \beta$, the adversary evaluates the correlation C using Proposition 1. For an idealized block cipher, C will be deviating from 0 with a probability of $1 - \frac{1}{\sqrt{2\pi}}2^{\frac{4-n}{2}}$ due to Proposition 2. Otherwise, $C = 0$ deterministically. The distinguishing test is simple and is defined as Algorithm 1. The applicability of Algorithm 1 is mainly limited to the cases with $k \geq n$ (i.e. where the key is longer than the block). Note that the error probability of distinguishing is negligible for all practical block sizes ($n \geq 32$).

Algorithm 1 Distinguisher for zero correlation

Require:

1. 2^{n-1} chosen plaintext-ciphertext pairs obtained with an (unknown) user-supplied key κ
2. Non-trivial zero-correlation linear hull $\alpha \nrightarrow \beta$

Perform:

1. Evaluate correlation C for the linear hull $\alpha \nrightarrow \beta$ using Prop. 1
2. If $C = 0$, then return *non-idealized*, else return *idealized*

Data complexity:
2^{n-1} chosen plaintext-ciphertext pairs
Computational complexity:
2^{n-1} evaluations of $\alpha \diamond x$ or $\beta \diamond y$
Success probability:
false positive probability $\frac{1}{\sqrt{2\pi}}2^{\frac{4-n}{2}}$ due to Prop. 2
false negative probability 0

Algorithm 1 relies on the existence of at least one non-trivial zero-correlation linear hull for the cipher attacked. In the following, we find zero-correlation linear hulls in some popular cipher constructions valid for any key value as well as propose key-recovery attacks based on Algorithm 1 and these zero-correlation linear hulls.

3 Zero-Correlation Linear Hulls

For a fixed key, an idealized cipher is a randomly drawn permutation which is likely to have at least one non-trivial linear approximation with correlation exactly 0. For instance, this can be observed if one takes the probability for a non-trivial linear approximation of a randomly drawn permutation to have zero correlation from Proposition 2 and recalls that nearly all of its 2^{2n} linear approximations are non-trivial. However, as every key value of the idealized cipher chooses another permutation from the set of all n-bit permutations and the choice is independent for different keys, which linear approximations have zero correlation will vary greatly from key to key for the idealized cipher.

On the contrary, for many real-world ciphers, there exist vast classes of non-trivial linear hulls with correlation zero, independently of the key value. In this section, we demonstrate non-trivial zero-correlation linear hulls for such popular cipher constructions as AES, balanced Feistel networks as well as Skipjack, CAST256, and CLEFIA. Additionally, we observe these linear hulls to have a correlation value of exactly 0 in our experiments with small-scale variants of ciphers.

3.1 Sufficient condition for zero correlation

Here we prove a sufficient condition for a linear hull of an iterative block cipher to have correlation zero. The proof is based on the notion of an incompatible pair of adjacent linear selection patterns. For a linear trail U of an iterative transform f, a pair of adjacent linear selection patterns u_{i-1} and u_i is called *incompatible* if the corresponding linear approximation $u_{i-1} \to u_i$ over the intermediate map f_i is zero, $C^{f_i}_{u_{i-1},u_i} = 0$ (see Subsection 1.2 and Figure 1 for the details of notation).

Proposition 3 (Sufficient condition for zero correlation). *If at least one pair of adjacent linear selection patterns is incompatible for every linear trail in a linear hull of an iterative transformation, the correlation of this linear hull is exactly 0.*

Proof. Recall the definition of a correlation contribution (2) of a trail and the theorem of linear trail composition (3) from Subsection 1.2. Due to (2), if $C^{f_i}_{u_{i-1},u_i} = 0$ at least for one linear approximation $u_{i-1} \to u_i$ over a round map f_i, the correlation contribution for this linear trail U is zero: $C_U = 0$. According to (3), putting $C_U = 0$ for every linear trail is sufficient for having a correlation C of exactly 0. The claim of the proposition follows.

Proposition 3 says that in order to prove that a linear hull over an entire iterative cipher has correlation zero, it is enough to locate a round map whose linear approximations always have correlation 0 in this linear hull.

3.2 Feistel-type block ciphers

Here we show zero-correlation linear hulls of several Feistel-type block ciphers [12, 20, 21, 24, 25] depicted in Figure 2. Similarly to impossible differentials, for showing zero-correlation linear hulls it is crucial to require the F-functions ϕ and ψ of these Feistel ciphers to be invertible.

Table 1. Zero-correlation linear hulls and best impossible differentials known. All Feistel constructions are assumed to have invertible F-functions

Block cipher construction	Impossible differential		Zero-correlation linear hull	
	rounds	pattern	rounds	pattern
Feistel	5	$(0, \Delta) \nrightarrow (\Delta, 0)$	5	$(a, 0) \nrightarrow (0, a)$
Skipjack	15 [25]	$(0, 0, 0, \Delta) \nrightarrow (\nabla, 0, 0, 0)$	15	$(0, 0, 0, a) \nrightarrow (b, 0, 0, b)$
CAST256	19 [7]	$(0, 0, 0, \Delta) \nrightarrow (\nabla, 0, 0, 0)$	18	$(0, 0, 0, a) \nrightarrow (0, a, 0, 0)$
CLEFIA	9 [26]	$(0, 0, 0, \Delta) \nrightarrow (0, 0, \Delta, 0)$ $(0, \Delta, 0, 0) \nrightarrow (\Delta, 0, 0, 0)$	9	$(a, 0, 0, 0) \nrightarrow (0, 0, 0, a)$ $(0, 0, a, 0) \nrightarrow (0, a, 0, 0)$
AES	4 [4]	$(\Theta, 0, 0, 0) \nrightarrow (\Theta', 0, 0, 0)$	4	$(\Gamma, 0, 0, 0) \nrightarrow (\Gamma', 0, 0, 0)$

$a \neq 0$, $b \neq 0$, $\Delta \neq 0$, $\nabla \neq 0$

AES: Θ, Θ', Γ, Γ' are 4-byte columns with exactly one nonzero byte; note that there are also other impossible differentials and zero-correlation linear hulls for AES

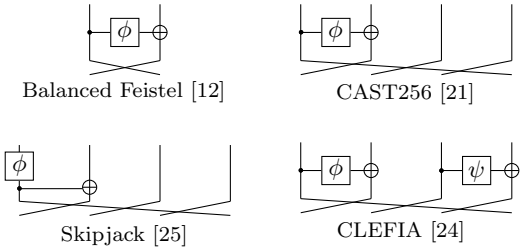

Fig. 2. Round maps of balanced Feistel network and some generalized Feistel-type constructions with F-functions ϕ and ψ invertible

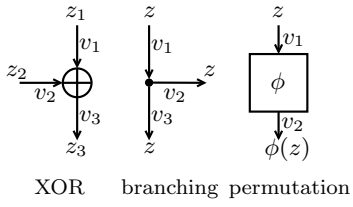

Fig. 3. Linear approximations of basic operations: XOR $\oplus$, branching $\bullet$, and permutation ϕ. Values z_1, z_2, and z_3 as well as linear selection patterns v_1, v_2, and v_3

Feistel ciphers make use of three basic operations: XOR-operation, branching operation, and a key-dependent F-function ϕ. Linear approximations over these operations comprise the linear trails of Feistel-type ciphers and obey three major rules (see also [19] and [1]):

Lemma 1 (XOR approximation [1]). *Either the three linear selection patterns at an XOR $\oplus$ are equal or the correlation over $\oplus$ is exactly zero.*

Proof. Consider the bitwise XOR operation with 2 input words z_1 and z_2 as well as 1 output word $z_3 = z_1 \oplus z_2$. Let (v_1, v_2) be the input selection pattern and v_3 the output selection pattern, see Figure 3. The probability of the linear approximation over the XOR operation to hold is then:

$$\begin{aligned} p^{\oplus}_{v_1,v_2,v_3} &= \Pr\{v_1 \diamond z_1 \oplus v_2 \diamond z_2 \oplus v_3 \diamond z_3 = 0\} \\ &= \Pr\{(v_1 \oplus v_3) \diamond z_1 = (v_2 \oplus v_3) \diamond z_2\}. \end{aligned}$$

Since the probability is computed over all z_1 and z_2, $p^{\oplus}_{v_1,v_2,v_3} \neq 1/2$ if and only if $v_1 \oplus v_3 = 0$ and $v_2 \oplus v_3 = 0$, simultaneously. This means that $v_1 = v_2 = v_3$ is necessary and sufficient for the linear approximation $(v_1, v_2) \to v_3$ to have a nonzero correlation over the bitwise XOR operation. By definition of correlation, the claim of the lemma follows.

Lemma 2 (Branching approximation [1]). *Either the three linear selection patterns at a branching point $\bullet$ sum up to 0 or the correlation over $\bullet$ is exactly zero.*

Proof. A branching point can be represented as a function with input z and output (z, z), see Figure 3. Again, if the input selection pattern is v_1 and the output selection pattern is (v_2, v_3), one has:

$$\begin{aligned} p^{\bullet}_{v_1,v_2,v_3} &= \Pr\{v_1 \diamond z \oplus v_2 \diamond z \oplus v_3 \diamond z = 0\} \\ &= \Pr\{(v_1 \oplus v_2 \oplus v_3) \diamond z = 0\}. \end{aligned}$$

The probability is computed over all inputs z and, therefore, $p^{\bullet}_{v_1,v_2,v_3} \neq 1/2$ if and only if $v_1 \oplus v_2 \oplus v_3 = 0$. Thus, the correlation over the branching point is nonzero, iff the three selection patterns sum up to 0.

Lemma 3 (Permutation approximation). *Over a permutation ϕ, if the input and output selection patterns are neither both zero nor both nonzero, the correlation over ϕ is exactly zero.*

Proof. Let ϕ be an invertible transform. Consider the linear approximation $v_1 \to v_2$ over ϕ, see Figure 3. If z is the input to ϕ, one has:

$$\begin{aligned} p^{\phi}_{v_1,v_2} &= \Pr\{v_1 \diamond z \oplus v_2 \diamond \phi(z) = 0\} \\ &= \begin{cases} \Pr\{v_2 \diamond \phi(z) = 0\}, & \text{if } v_1 = 0, \\ \Pr\{v_1 \diamond z = 0\}, & \text{if } v_2 = 0. \end{cases} \end{aligned}$$

In case $v_1 \neq 0$ and $v_2 = 0$, $p^{\phi}_{v_1,v_2} = 1/2$, since it is computed over all z. In case $v_1 = 0$ and $v_2 \neq 0$, $p^{\phi}_{v_1,v_2} = 1/2$, since ϕ is bijective and $\phi(z)$ takes all values. By definition of correlation, the claim of the lemma follows.

The interpretation of Lemmata 1 to 3 is as follows. If in a linear trail:

- the selection patterns at XOR $\oplus$ are not equal,
- the selection patters at branching point $\bullet$ do not sum up to zero, or
- the selection patterns at permutation ϕ are neither both zero nor both nonzero,

then this linear trail contains an incompatible pair of adjacent selection patterns. If an incompatible pair of adjacent selection patterns can be shown for each linear trail in a linear a hull, the sufficient condition of Proposition 3 applies, which is performed in the proof of

Theorem 1 (Zero-correlation linear hulls for Feistel ciphers). *If the underlying F-functions of the Feistel-type construction are invertible, the following linear hulls have zero correlation for $a \neq 0$ and $b \neq 0$:*

- $(a, 0) \nrightarrow (0, a)$ *for 5 rounds of balanced Feistel ciphers,*
- $(a, 0, 0, 0) \nrightarrow (0, 0, 0, a)$ *and* $(0, 0, a, 0) \nrightarrow (0, a, 0, 0)$ *for 9 rounds of CLEFIA-type ciphers,*
- $(0, 0, 0, a) \nrightarrow (b, 0, 0, b)$ *for 15 rounds of Skipjack-type ciphers, and*
- $(0, 0, 0, a) \nrightarrow (0, a, 0, 0)$ *for 18 rounds of CAST256-type ciphers.*

Proof. For each of these Feistel-type ciphers, we proceed as follows. Starting separately with the input and output selection patterns of a linear hull, we obtain partial linear trails with a nonzero correlation contribution using Lemmata 1 to 3. After that, we demonstrate that both partial trails cannot match in the middle without turning the correlation contribution of each of the trails to 0. This makes Proposition 3 applicable and proves that the correlation of the linear hull is exactly 0.

Balanced Feistel. Consider 5 rounds of the balanced Feistel cipher with bijective F-functions with input and output selection patterns $(a, 0)$ and $(0, a)$, respectively, see Figure 4, and try to construct linear trails without incompatible adjacent selection patterns using Lemmata 1 to 3. The F-functions of rounds 1 and 5 have zero input and output selection patterns due to Lemmata 1 and 3. Due to Lemma 2, the selection patterns after round 1 and before round 5 are just swapped input and output selection patterns. The F-functions of rounds 2 and 4 have nonzero input selection patterns due to Lemma 2. At round 3, Lemma 1 makes the output selection pattern of the F-function nonzero. At the same time, Lemma 2 yields a zero input selection pattern for the F-function in this round. Hence, by Lemma 3 the pair of adjacent selection patterns at round 3 is incompatible for each linear trail of the linear hull.

CLEFIA, Skipjack, CAST256. For the linear hulls specified for 9 rounds of CLEFIA, 15 rounds of Skipjack and 18 rounds of CAST256, the corresponding linear trails are derived in Figures 5, 6, and 7 using the lemmata above and all have at least one incompatible pair of adjacent selection patterns. In each linear trail, the linear approximation over rounds 5, 6, and 12 of these constructions, correspondingly, exhibit correlation 0. For CLEFIA and CAST256, the incompatible selection patterns at the input and output of these round maps are of the same type as for the balanced Feistel. For Skipjack, Lemma 2 provides an incompatible pair of adjacent selection patterns.

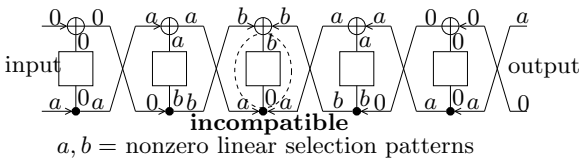

Fig. 4. Zero-correlation linear hull $(a, 0) \nrightarrow (0, a)$ over 5 rounds of balanced Feistel cipher with bijective F-functions: each linear trail exhibits an incompatible pair of adjacent selection patterns at round 3 due to Lemma 3

Applying Proposition 3 to the incompatible pairs of adjacent selection patterns above yields the claims of the theorem.

Theorem 1 demonstrates that several widely used Feistel-type block cipher constructions have zero-correlation linear hulls when instantiated with bijective F-functions. We experimentally verified the correctness of Theorem 1 on small-scale balanced Feistel, CLEFIA, Skipjack, and CAST256 ciphers. The findings are summarized and compared to impossible differentials in Table 1.

Luby and Rackoff [18] proved the resistance of the balanced Feistel cipher with random F-functions to all adaptive chosen plaintext attacks for 3 rounds and to all adaptive chosen plaintext and ciphertext attacks for 4 rounds, if the number of queries the adversary is allowed to make is $\ll 2^{n/2}$. Our 5-round zero-correlation linear hull for balanced Feistel does not contradict to these results, since, on the one hand, the adversary requires at least 2^{n-1} cipher queries to detect the zero correlation property and, on the other hand, the F-functions have to be bijective for Theorem 1 to hold.

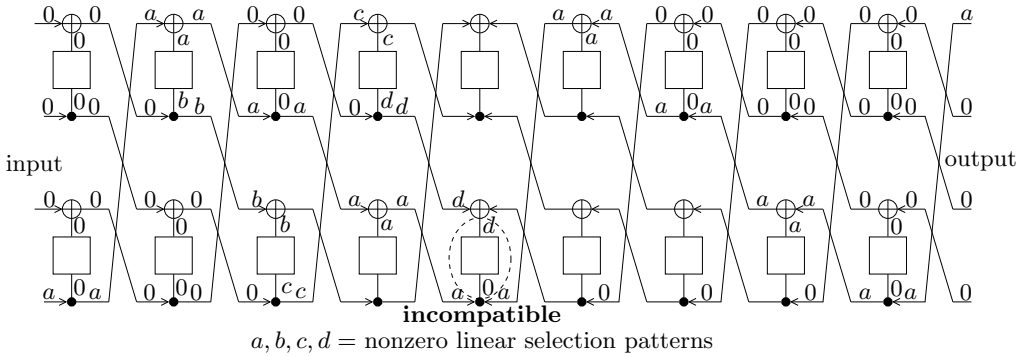

Fig. 5. 9-round zero-correlation linear hull $(a, 0, 0, 0) \nrightarrow (0, 0, 0, a)$ for CLEFIA-type ciphers (type-II generalized Feistel network) with bijective F-functions

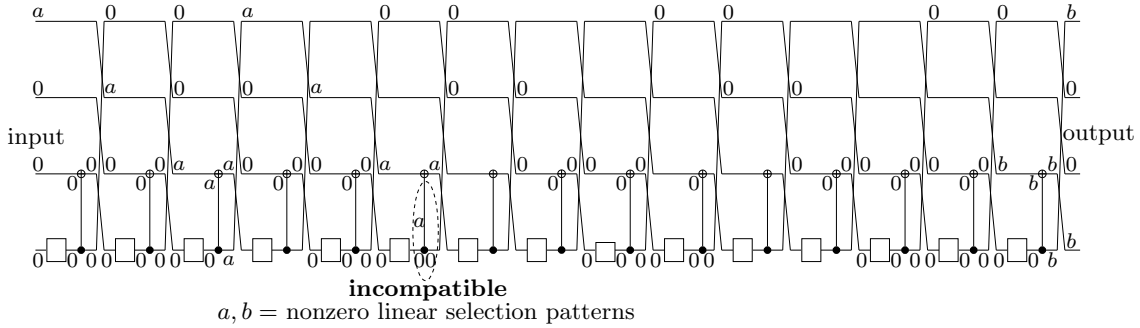

Fig. 6. 15-round zero-correlation linear hull $(0,0,0,a) \nrightarrow (b,0,0,b)$ for Skipjack-type ciphers with bijective F-functions

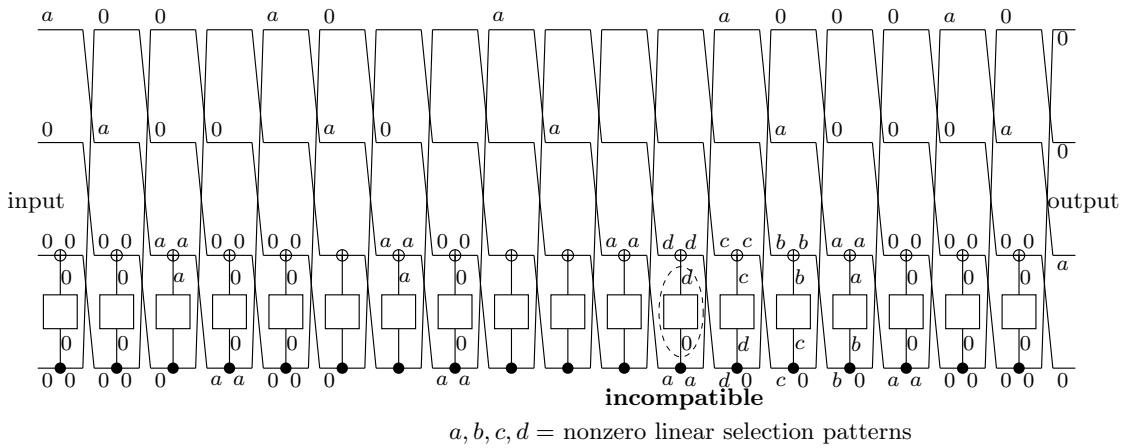

Fig. 7. 18-round zero-correlation linear hull $(0,0,0,a) \nrightarrow (0,a,0,0)$ for CAST256-type ciphers with bijective F-functions

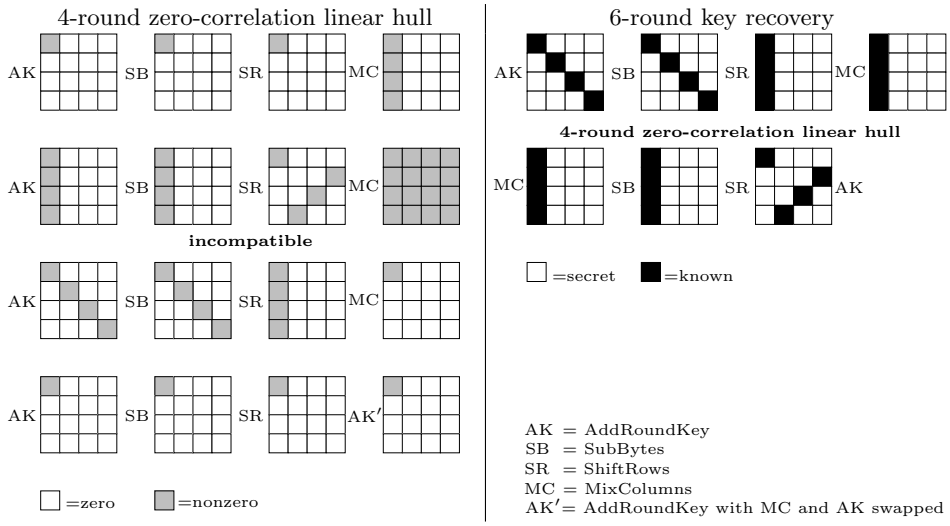

Fig. 8. Zero-correlation linear cryptanalysis of AES-192 and AES-256: 4-round zero-correlation linear hull (linear selection patterns on the left) and 6-round key recovery (cipher state on the right)

3.3 Advanced Encryption Standard (AES)

Here we show a class of zero-correlation linear hulls for 4 rounds of AES. The proof is based on checking the forward and backward diffusion properties as well as on the application of Proposition 3.

We consider a 4-round AES transform which consists of the initial key addition followed by 3 full AES rounds and one incomplete round without the MixColumns transformation, see Figure 8. One full AES round comprises SubBytes (SB), ShiftRows (SR), MixColumns (MC), and AddRoundKey (AK) operations. The last incomplete round consists of SubBytes (SB), ShiftRows (SR) as well as the AddRoundKey operation (AK') with the round key mapped using the inverse MixColumns MC^{-1}.

Theorem 2 (Zero-correlation linear hulls for AES). *Let Γ and Γ' be 4-byte column selection patterns with exactly one nonzero byte. Then each of the linear hulls $(\Gamma, 0, 0, 0) \nrightarrow (\Gamma', 0, 0, 0)$ over 4 AES rounds has zero correlation.*

Proof. A nonzero byte of a linear selection pattern is called an *active byte* in the sequel. For AES, due to the forward diffusion, any input selection pattern with only a single active byte necessarily results in a selection pattern with all 16 active bytes after 2 full rounds. At the same time, following the backward diffusion from the output selection pattern over one incomplete round and one full round, any output selection pattern with only one active byte results in exactly one active diagonal (4 active bytes). Hence, every pair of adjacent selection patterns in this linear hull over the key addition of round 2 is incompatible by Lemma 3 (for a fixed key, the byte key addition is an invertible map). By Proposition 3, the latter directly translates to a 4-round zero-correlation linear hull. See Figure 8 for an example of an zero-correlation linear hull of this type.

Theorem 2 yields a class of zero-correlation linear hulls for 4 rounds of AES. Note that AES has also further zero-correlation linear hulls of similar types over 4 rounds. We

verified the incompatibility of adjacent linear selection patterns of linear trails in the linear hull of Theorem 2 in our experiments with small-scale SPNs.

4 Zero-Correlation Key Recovery

Algorithm 1 of Section 2 provides a distinguisher for a block cipher when a linear hull with a correlation of exactly 0 is given. Theorems 1 and 2 of Section 3 show numerous zero-correlation linear hulls in many popular cipher constructions, whose input and output selection patterns are independent of the key value. In this section, we turn this into a key recovery for round-reduced AES-192, AES-256, and CLEFIA-256 [13], [24].

To perform key recovery over more rounds than covered by the zero-correlation linear hull, one has to guess the (sub)key bits that are needed to compute the internal *values* chosen by the input and output selection patterns of the linear hull from a plaintext and a ciphertext. This is a major distinctive feature of zero-correlation linear cryptanalysis compared to impossible differential cryptanalysis, where the adversary has to guess key to control the *difference* propagation up to the boundaries of the impossible differential. Moreover, a control over the type of differences is sufficient and the knowledge of the exact difference values is not needed. That is, the number of rounds that can be attacked by zero-correlation linear cryptanalysis is defined by the form and length of the zero-correlation linear hull itself and by the diffusion properties of the cipher.

Another crucial difference between zero-correlation cryptanalysis and impossible differential cryptanalysis is the following. For a key guess, once the adversary has a pair of texts with an impossible combination of input and output differences, he can deduce that this key guess is wrong, since the attacked cipher would not allow the impossible differential to go though. For this, only a subset of all plaintext-ciphertext pairs might be needed. In the zero-correlation cryptanalysis, the adversary has to perform an exact evaluation of correlation to tell if the key guess results in a zero-correlation linear hull. Here a full codebook or at least a half of it (see Proposition 1) is always required. This basically reduces the applicability of zero-correlation cryptanalysis to block ciphers whose key is longer than the block.

4.1 6 Rounds of AES-192 and AES-256

The zero-correlation linear hull of Theorem 2 and Figure 8 over 4 rounds of AES can be turned into a key recovery against 6 rounds of AES-192 and AES-256. The general procedure is to partially encrypt each plaintext and to partially decrypt the corresponding ciphertext with a guess of subkey bits. For each guess, one computes the relevant parts of the intermediate internal state and verifies if the remaining cipher exhibits the zero-correlation linear hull. The key-recovery attack can be outlined as follows:

1. Guess the first diagonal of the first subkey and the main diagonal of round-6 subkey (8 bytes, see Figure 8). For each guess:

   (a) Partially encrypt each of the 2^{128} plaintexts one round forwards and partially decrypt each of the corresponding 2^{128} ciphertexts one round backwards.
   (b) Evaluate the correlation for two zero-correlation linear hulls of the type given in Figure 8 with input selection pattern in the first column. The right guess will have zero correlation for both linear hulls.
2. Guess the second diagonal of the first subkey (4 bytes). The main diagonal of round-6 subkey is already known from Step 1. For each guess:
   (a) Partially encrypt each of the 2^{128} plaintexts one round forwards and partially decrypt each of the corresponding 2^{128} ciphertexts one round backwards.
   (b) Evaluate the correlation for the zero-correlation linear hull with input selection pattern in the second column. The right guess will have zero correlation.
3. Guess the third diagonal of the first subkey (4 bytes). The main diagonal of round-6 subkey has already been determined in Step 1. For each guess:
   (a) Partially encrypt each of the 2^{128} plaintexts one round forwards and partially decrypt each of the corresponding 2^{128} ciphertexts one round backwards.
   (b) Evaluate the correlation for the zero-correlation linear hull with input selection pattern in the third column. The right guess will have zero correlation.
4. Guess the remaining bits of the user-supplied key (of which the determined diagonals of the first subkey are a part) by brute force using at most two plaintext-ciphertext pairs.

Once the one diagonal of the first subkey has been determined (Step 1), we switch to active bytes in another column of the input selection pattern for the zero-correlation linear hull and repeat the procedure (Steps 2 and 3). We use two more input selection patterns corresponding to two more diagonals of the first subkey. For each of these, we do not have to guess another diagonal of the last subkey and just stick to the previous output selection pattern of the zero-correlation linear hull.

For each of 2^{64} guesses in Step 1, one needs to evaluate the correlation values for two linear hulls to decrease the error probability. Due to Proposition 2, we expect a wrong guess to result in zero correlation value with probability about $2^{-63.3}$. For the correlations of two distinct linear hulls, this probability reduces to a negligible value of about $2^{-126.7}$. The evaluation of the correlation for another linear hull can be performed in parallel.

The complexity of each of Steps 2 and 3 is about $2^{32} \cdot 2^{128}/12 \approx 2^{156.4}$ encryptions. The complexity of Step 4 is $2 \cdot 2^{256-64-2 \cdot 32} = 2^{161}$ encryptions. Thus, the computational complexity of the full 6-round attack is dominated by Step 1 and can be estimated as $2^{64} \cdot 2^{128}/12 \approx 2^{188.4}$ encryptions and is the same for both AES-192 and AES-256. The data complexity is 2^{128} plaintext-ciphertext pairs (cf. e.g. $2^{118.8}$ time and $2^{2^{113.8}}$ data to attack 7 rounds of AES-192 as well as $2^{227.8}$ time and $2^{111.1}$ data complexity to attack 8 rounds of AES-256 in [16] with an impossible-differential key recovery). A similar 5-round chosen-ciphertext or chosen-plaintext attack would reduce the computational complexity to about $2^{156.3}$ encryptions and the data requirements to 2^{127}.

4.2 13 rounds of CLEFIA-256

Based on the zero-correlation linear hull $(a, 0, 0, 0) \nrightarrow (0, 0, 0, a)$ of Theorem 1, Table 1, and Figure 5 over 9 rounds for CLEFIA-type structures, we demonstrate a

zero-correlation key-recovery attack against 13 rounds of CLEFIA-256. The general procedure is similar to that for the attack on AES: We guess all key values needed to compute the active intermediate values at the input and output selection patterns of the zero-correlation linear hull. In our attack, the 9-round zero-correlation linear hull covers rounds 3 to 11. The procedure can be outlined as follows:

1. Guess 4 32-bit secret-key values:
   - The XOR of the 32-bit round-key chunk and 32-bit whitening-key chunk in round 1 to predict the output of one F-function in round 1,
   - The 32-bit round-key chunk to predict the output of one F-function in round 2,
   - The XOR of the 32-bit round-key chunk and 32-bit whitening-key chunk in round 12 to predict the input of one F-function in round 12,
   - The 32-bit round-key chunk to predict the input of one F-function in round 13.
2. For each guess:
   (a) Partially encrypt each of 2^{128} plaintexts two rounds forwards and partially decrypt each of the corresponding 2^{128} ciphertexts two rounds backwards.
   (b) Evaluate the correlation for three zero-correlation linear hulls of the type given in Figure 5. The right guess will have zero correlation for all three linear hulls.

We evaluate correlation for three distinct linear hulls to reduce the error probability for each of 2^{128} guesses to about 2^{-190}. The computational complexity of the 13-round attack amounts to $2^{128} \cdot 2^{128} \cdot \frac{2}{13} \approx 2^{253.3}$ encryptions. The data complexity is 2^{128} plaintext-ciphertext pairs (cf. 2^{212} time and $2^{120.3}$ data in [26] for a 14-round impossible differential key-recovery attack on CLEFIA-256). A similar 11-round chosen-ciphertext or chosen-plaintext attack would have a computational complexity of about $2^{155.5}$ encryptions and a data complexity of 2^{127} texts.

5 Conclusion

In this article, we have introduced a novel extension of linear cryptanalysis – zero-correlation linear cryptanalysis. We demonstrate linear hulls with a correlation of exactly 0 for many cipher structures including AES as well as balanced and generalized Feistel networks (CLEFIA, Skipjack, and CAST256). This extension of linear cryptanalysis bears some similarities to impossible differential cryptanalysis and can be seen as its counterpart in the domain of linear cryptanalysis, though being essentially different and having numerous significant distinctions.

We apply zero-correlation linear cryptanalysis to 6 rounds of AES-192 and AES-256 as well as 13 rounds of CLEFIA-256. The new attack does not break stronger ciphers than the impossible-differential attack. This conforms to the general belief that for most ciphers (however, not for all of them), differential attacks are stronger than linear attacks. The main contribution of this work belongs to the theory of cryptanalysis of block ciphers. One may expect some block ciphers to be re-evaluated using the novel approach to linear cryptanalysis. This attack also can be taken into account while designing new block ciphers.

References

1. E. Biham. On Matsui's Linear Cryptanalysis. In *EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 341–355. Springer, 1995.
2. E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In *EUROCRYPT'99*, LNCS, pages 12–23. Springer, 1999.
3. E. Biham, O. Dunkelman, and N. Keller. Related-Key Impossible Differential Attacks on 8-Round AES-192. In *CT-RSA'06*, LNCS, pages 21–33. Springer-Verlag, 2006.
4. E. Biham and N. Keller. Cryptanalysis of Reduced Variants of Rijndael, 1999. Available online at `www.madchat.fr/crypto/codebreakers/35-ebiham.pdf`.
5. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *CRYPTO'90*, LNCS, pages 2–21. Springer-Verlag, 1990.
6. J. Borst, L. R. Knudsen, and V. Rijmen. Two Attacks on Reduced IDEA. In *EUROCRYPT'97*, LNCS, pages 1–13. Springer-Verlag, 1997.
7. J. Choy and H. Yap. Impossible Boomerang Attack for Block Cipher Structures. In *IWSEC'09*, LNCS, pages 22–37. Springer-Verlag, 2009.
8. J. Daemen and V. Rijmen. *The Design of Rijndael: AES – The Advanced Encryption Standard*. Springer-Verlag, 2002.
9. J. Daemen and V. Rijmen. Probability Distributions of Correlation and Differentials in Block Ciphers. *Journal of Mathematical Cryptology*, 1(3):221–242, 2007.
10. O. Dunkelman and N. Keller. An Improved Impossible Differential Attack on MISTY1. In *ASIACRYPT'08*, LNCS, pages 441–454. Springer-Verlag, 2008.
11. J. Etrog and M. J. B. Robshaw. On Unbiased Linear Approximations. In *ACISP'10*, volume 6168 of *LNCS*, pages 74–86. Springer, 2010.
12. H. Feistel. Cryptography and Computer Privacy. *Scientific American*, 228:15–23, 1973.
13. FIPS. Advanced Encryption Standard. Publication 197. National Bureau of Standards, U.S. Department of Commerce, 2001.
14. P. Junod. On the Complexity of Matsui's Attack. In *SAC'01*, LNCS, pages 199–211. Springer-Verlag, 2001.
15. L. R. Knudsen and J. E. Mathiassen. A Chosen-Plaintext Linear Attack on DES. In *FSE'00*, LNCS, pages 262–272. Springer-Verlag, 2000.
16. J. Lu, O. Dunkelman, N. Keller, and J. Kim. New Impossible Differential Attacks on AES. In *INDOCRYPT'08*, LNCS, pages 279–293. Springer-Verlag, 2008.
17. J. Lu, J. Kim, N. Keller, and O. Dunkelman. Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. In *CT-RSA'08*, LNCS, pages 370–386. Springer-Verlag, 2008.
18. M. Luby and C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.
19. M. Matsui. Linear Cryptoanalysis Method for DES Cipher. In *EUROCRYPT'93*, LNCS, pages 386–397. Springer-Verlag, 1993.
20. A. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
21. S. Moriai and S. Vaudenay. On the Pseudorandomness of Top-Level Schemes of Block Ciphers. In *ASIACRYPT'00*, volume 1976 of *LNCS*, pages 289–302. Springer-Verlag, 2000.
22. K. Nyberg. Linear Approximation of Block Ciphers. In *EUROCRYPT'94*, LNCS, pages 439–444. Springer-Verlag, 1994.
23. L. O'Connor. Properties of Linear Approximation Tables. In *FSE'94*, LNCS, pages 131–136. Springer-Verlag, 1994.
24. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In *FSE'07*, LNCS, pages 181–195. Springer-Verlag, 2007.
25. J. Sung, S. Lee, J. I. Lim, S. Hong, and S. Park. Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis. In *ASIACRYPT'00*, volume 1976 of *LNCS*, pages 274–288. Springer-Verlag, 2000.
26. Y. Tsunoo, E. Tsujihara, M. Shigeri, T. Saito, T. Suzaki, and H. Kubo. Impossible Differential Cryptanalysis of CLEFIA. In *FSE'08*, LNCS, pages 398–411. Springer-Verlag, 2008.
27. S. Vaudenay. Decorrelation: A Theory for Block Cipher Security. *J. Cryptology*, 16(4):249–286, 2003.