On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers

Céline Blondeau[1], Andrey Bogdanov[2], and Meiqin Wang[3]

[1] Department of Information and Computer Science, Aalto University School of Science, Finland
celine.blondeau@aalto.fi
[2] Technical University of Denmark, Denmark
anbog@dtu.dk
[3] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
mqwang@sdu.edu.cn

Abstract. For many word-oriented block ciphers, impossible differential (ID) and zero-correlation linear (ZC) cryptanalyses are among the most powerful attacks. Whereas ID cryptanalysis makes use of differentials which never occur, the ZC cryptanalysis relies on linear approximations with correlations equal to zero. While the key recovery parts of ID and ZC attacks may differ and are often specific to the target cipher, the underlying distinguishing properties frequently cover the same number of rounds. However, in some cases, the discrepancy between the best known IDs and ZC approximations is rather significant.

At EUROCRYPT'13, a link between these two distinguishers has been presented. However, though being independent of the underling structure of the cipher, it is usually not useful for most known ID or ZC distinguishers. So despite the relevance of those attacks, the question of their equivalence or inequivalence has not been formally addressed so far in a constructive practical way.

In this paper, we aim to bridge this gap in the understanding of the links between the ID and ZC properties. We tackle this problem at the example of two wide classes of ciphers, namely, Feistel- and Skipjack-type ciphers. As our major contribution, for those ciphers, we derive conditions for impossible differentials and zero-correlation approximations to cover the same number of rounds. Using the conditions, we prove an equivalence between ID and ZC distinguishers for type-I and type-II Feistel-type ciphers, for Rule-A and Rule-B Skipjack-type ciphers, as well as for TWINE and LBlock. Moreover, we show this equivalence for the Extended Generalised Feistel construction presented at SAC'13. We also use our theoretical results to argue for an inequivalence between ID and ZC distinguishers for a range of Skipjack-type ciphers.

Keywords: impossible differential, zero-correlation, Feistel-type ciphers, Skipjack-type ciphers.

I. Boureanu, P. Owesarski, and S. Vaudenay (Eds.): ACNS 2014, LNCS 8479, pp. 271–288, 2014.
© Springer International Publishing Switzerland 2014

1 Introduction

Differential and linear cryptanalyses [3,14] definitely belong to the most essential types of attacks on block ciphers and have known numerous generalizations and extensions. Among those are impossible differential (ID) cryptanalysis [2,12] and zero-correlation (ZC) cryptanalysis [8,9] which have been proven efficient when applied to word-oriented block ciphers – block ciphers with strong local diffusion.

Classically, *ID distinguishers* take advantage of differentials which never occur for the studied permutations. This technique has been the subject of many research publications. The security of new and old primitives has been evaluated with respect to this attack. For instance, an early ID attack still remains the best known key-recovery for Skipjack [2]. Also automated methods to find IDs have been proposed [13, 25].

In *ZC cryptanalysis*, attackers rather take advantage of linear approximations that have probability 1/2 to hold. This new attack which can be seen as multidimensional linear attack with capacity equal to zero [7], has also been applied to many word-oriented block ciphers [6, 7, 9, 18, 23, 24] to evaluate their security and often improve upon the state-of-the-art cryptanalysis.

Usually techniques similar to the $\mathcal{U}$-method or a generalization thereof are used to identify ID distinguishers for word-oriented construction. In the following, we refer to these various methods as *matrix methods*. Recently, it has been shown in [18] that this method can be applied to find ZC distinguishers in particular for the block cipher LBlock [26].

While for many of these ciphers the discovered ZC distinguishers cover the same number of rounds as the ID distinguishers, the numbers of rounds covered by the properties can be sometimes rather distinct. In [7], there is a ZC distinguisher for a 30-round Skipjack variant for which only a 21-round ID distinguisher is known to exist. This discrepancy raises the *question of equivalence between ZC and ID distinguishers*. As a first attempt to formalize this problem, at EUROCRYPT'13 [4], using a mathematical link between linear and differential cryptanalysis, this question has been shown to have a positive answer in the special case of multidimensional linear spaces of specific size. The link of [4] can be outlined as follows:

For a given n-bit block cipher, we have an ID distinguisher $(0, \delta) \nrightarrow (0, \gamma)$ with $\delta \in \mathbb{F}_2^t \setminus \{0\}$ and $\gamma \in \mathbb{F}_2^{n-t} \setminus \{0\}$ if and only if we have a ZC distinguisher $(u, 0) \nrightarrow (v, 0)$ with $u \in \mathbb{F}_2^{n-t} \setminus \{0\}$ and $v \in \mathbb{F}_2^t \setminus \{0\}$. Though this relation is independent of the underlying cipher and its specific structure, it has the limitation of involving $(2^t - 1)(2^{n-t} - 1) \approx 2^n$ differentials or linear approximations. However, for many ciphers, fewer differentials are involved, which poses a limitation to the practical application of this general theoretical result.

In this paper, with matrix techniques for IDs and ZC approximations, we address this question for many more relevant constructions including Feistel-type and Skipjack-type ciphers. A major difference of this paper with the link of [4] is that the results presented here depend of the structure of the underlying ciphers, thus, being both less general and more practical.

Our Contributions. The contributions of this paper are as follows.

- **Condition of equivalence between ZC and ID distinguishers:** As our main contribution, we show that for many constructions, once we have an ID distinguisher on r rounds involving M differentials, we obtain a ZC distinguisher on the same r rounds involving M linear approximations, and vise versa. This yields a necessary and sufficient condition of equivalence between ZC and ID distinguishers. We point out that the key recovery procedures on top of those distinguishers may be quite different and may result in different number of rounds cryptanalyzed in the actual attacks. While for most Feistel constructions, the inverse of the internal function is not required for deciphering, for ciphers like Skipjack the deciphering is obtained thanks to the inverse of the internal function. We refer to the first type as *Feistel-type* ciphers and to the second type as *Skipjack-type* ciphers. Understanding the relation between these distinguishers, ID and ZC, will help designers check if a separate study of ZC and ID distinguishers is necessary for a security evaluation. Representation of the different constructions can be found in the different part of this paper. For instance, in Fig. 1, Feistel-type ciphers are represented, and in Fig. 3 and Fig. 4 Skipjack-type ciphers are represented.
- **Inequivalence considerations for ZC and ID distinguishers:** The necessary and sufficient equivalence condition also allows us to reason about cases of inequivalence for Feistel- and Skipjack-type ciphers. We consider inequivalence between ZC and ID distinguishers for several interesting examples including the Feistel-type constructions of FSE'10 [19] featuring optimal branch shuffles as well as for the construction proposed at SAC'13 [1]. We also explain the type of inequivalence between ID and ZC distinguishers observed for Skipjack variants in ASIACRYPT'12 [7].

Organization of the Paper. The remainder of this paper is organized as follows. In Section 2, we define what we call a Feistel-type cipher and recall how a matrix representation of the round function can be used to find ID distinguishers or to compute the differential diffusion of such constructions. In the same section, we also reconsider the recent method proposed in [18] to find ZC distinguishers on a Feistel-type cipher. Based on this method, in Section 3, we present conditions under which ID distinguishers involving M differentials and ZC ones involving M linear approximations can be applied on the same number of rounds of a Feistel-type cipher. Section 4 is dedicated to the Skipjack-type ciphers. In this section, we discuss the equivalence/inequivalence between ZC and ID distinguishers on Skipjack variants. In Section 5, we discuss the adaption of the results of Section 3 and Section 4 to other types of word-oriented ciphers. In particular, we discuss the Extended Generalised Feistel construction presented at SAC'13 [1] and constructions similar to MARS and GF-NLFSR such as Four-Cell. Section 6 concludes this paper.

2 Preliminaries

In this paper we assume word-oriented block ciphers with b words. The state of a n-bit word-oriented block cipher with $n = b \cdot s$ is represented by $X = (X_1, X_2, \cdots, X_b)$ where the X_i, $1 \leq i \leq b$ are blocks or words of s bits.

As recalled in the introduction, different constructions make use of this block decomposition of the state, to apply at each round non-linear operations on a subset of these blocks. Impossible differential cryptanalysis and zero-correlation linear cryptanalysis are among the best attacks on this type of construction. In this section, we describe these two distinguishers and their relation on what we call a Feistel-type cipher.

2.1 Feistel-Type Cipher and Matrix Representation

At FSE'10 [19], Suzaki and Minematsu proposed a general framework to describe what we call in this paper a Feistel-type cipher. This framework covers the well known type-I (see Fig. 1), type-II, type-III (similar to type-I) constructions as well as constructions such as the one proposed by Nyberg in [16]. The round function of Feistel-type cipher is such that a branch (word) can at each round be the input of a non-linear function or be linearly affected by the output of such non-linear function. As represented[1] in Fig. 1, a branching operation is done on the branches corresponding of the input of a non-linear function, and an exclusive-or addition (Xor) is done on the branches modified by the output of these non-linear functions. The number I of non-linear layers depends on the construction and can vary from 1 to $b/2$. Part of the diffusion is then provided by a permutation of the branches. For such constructions, a key is usually Xor-ed

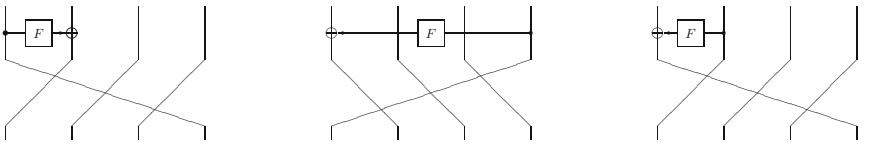


Fig. 1. A type-I Feistel with 4 branches: On the left the round function, in the middle the inverse of the round function and on the right the mirror of the round function as described in Def. 2.

to the partial state. As the distinguishers presented in this paper do not depend on this operation, this part will not be described.

Notice that given the round function of a Feistel-type cipher, as for a SPN constructions, one can distinguish the non-linear part consisting of the application of the non-linear functions to the linear part, consisting on the permutation of the branches. Similarly to what has been done in [1], the round function of a

[1] While depending on the construction, the number of branches of a word-oriented cipher can varies, for illustration purposes the pictures presented in this paper concentrate on ciphers with 4 branches.

Feistel-type cipher can be matricially represented. This description can be split in regard to the different layers which are F-layer and P-layer.

Definition 1. *Omitting key and constant addition, the round function of a Feistel-type cipher with b branches can be matricially represented as a combination of two $b \times b$ matrices $\mathcal{F}$, $\mathcal{P}$ with coefficients $\{0, 1, F_i\}$ where the $\{F_i\}_{i \leq I}$ denote the internal non-linear functions.*

- *Representing the non-linear layer (F-layer), the non-zero coefficients of the matrix $\mathcal{F}$ are equal to 1 in the diagonal and have coefficient F_i in row j and column k if the input of the function F_i is given by the k-th branch and the output is Xor-ed to the j-th branch. Meaning that $\mathcal{F}$ can have up to one F_i on each row and column.*
- *Representing the permutation of the branches (P-layer), the matrix $\mathcal{P}$ is a permutation matrix with only one non-zero coefficient per line and column.*

From these two matrices, a Feistel-type round function can be represented by a $b \times b$ matrix $\mathcal{R}$ as $\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$.

Example 1. The round function of the Type-I Feistel with 4 branches depicted in Fig. 1 can be represented from $\mathcal{F}$ and $\mathcal{P}$ as follows:

$$\mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ F & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{P} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \text{and } \mathcal{R} = \mathcal{P} \cdot \mathcal{F} = \begin{pmatrix} F & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

In this paper, we assume that the internal non-linear functions $F_i : \mathbb{F}_2^s \to \mathbb{F}_2^s$, are bijective. When it is not necessary, to make a distinction between the different non-linear functions, we denote them as F instead of F_i.

In this paper, -1 and $-F$ are identified with respectively 1 and F. The matrix representation of the inverse round function is $\mathcal{R}^{-1} = \mathcal{F}^{-1} \cdot \mathcal{P}^{-1}$.

2.2 Matrix Method for Impossible Differential Distinguisher

Through this paper, we express a truncated input (resp. output) difference as a vector Δ (resp. Γ) of size b.

Impossible differential distinguishers are often derived from a miss-in-the-middle or inconsistency between two intermediate differences. More precisely, cryptanalysts are interested in finding truncated differences Δ and Γ and some integers ℓ and m such that we have an inconsistency between the intermediate differences $\mathcal{R}^{\ell} \cdot \Delta$ and $\mathcal{R}^{-m} \cdot \Gamma$.

To study the propagation of differences thought this type of construction, the rules depicted in Fig. 2 and the matrix representation of the round function of a Feistel-type cipher are used. In particular one can find ID by computing the values $\mathcal{R}^{\ell} \cdot \Delta$ and $\mathcal{R}^{-m} \cdot \Gamma$ and detecting an inconsistency between the intermediate differences. This method has been described in [11,13] and used to analyse the security of many ciphers.

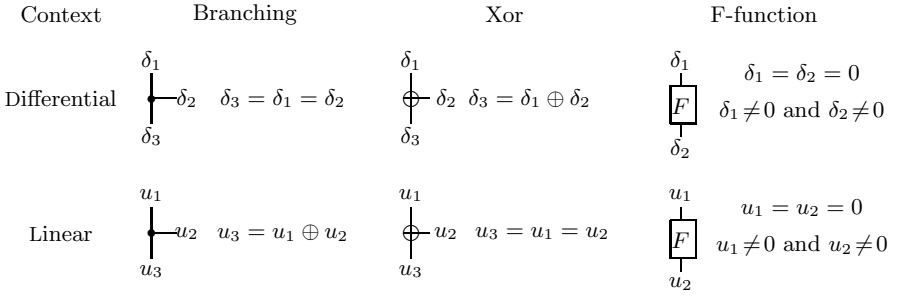


Fig. 2. Propagation of differences and linear masks through the basic operations. δ_1, δ_2, δ_3 denote differences and u_1, u_2, u_3 linear masks. The conditions correspond to the case where the probabilities/correlations are non-zero.

2.3 Matrix Method for Zero-Correlation Distinguishers

While ID cryptanalysis has been defined at the end of the 90's, the first attack using linear approximations with no-correlation has been published in 2012 [9].

Through this paper, we denote a truncated input (resp. output) mask as a vector U (resp. V) of size b. As for ID cryptanalysis, the classical method used to find ZC approximations consists in detecting an inconsistency, a difference, between two intermediate masks.

In [18] a generic method to find zero-correlation linear approximations on Feistel-type ciphers is described. This method is similar to the matrix method used for finding impossible differentials. Nevertheless, as depicted in Fig. 2, the branching and Xor operations in the linear context and then a fortiori for ZC distinguishers are converse to the ones in the differential context.

From these simple observations, we deduce that the matrix representation of the round function can not be used directly to find ZC distinguishers. Instead, as in [18] it seems natural to define what we will call the mirror round function. In this mirror function as illustrated in Fig. 1 the role played by the input and output of the non-linear functions are swapped meaning that the branching and Xor operations are swapped.

The matrix representation of what we call mirror function of a Feistel-type cipher can be defined easily from the matrix representation of the original function.

Definition 2. *For a Feistel-type cipher given the matrix representation of the round function $\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$, we call mirror function the round function described by the matrix $\mathcal{M} = \mathcal{P} \cdot \mathcal{F}^T$, where $\mathcal{F}^T$ denotes the transposition of the matrix $\mathcal{F}$.*

Example 2. The mirror function of the Feistel-type function of Fig. 1 can be represented by the matrix

$$\mathcal{M} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & F & 0 & 0 \end{pmatrix} \text{ with inverse } \mathcal{M}^{-1} = \begin{pmatrix} F & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Description of the matrix method in the ZC context [18] is given from the mirror of the round function of the LBlock cipher. In a general matter, as in the differential context, we can use this method to determine the linear diffusion of the cipher or to find ZC distinguishers on a Feistel-type cipher.

3 Equivalence for Feistel-Type Ciphers

3.1 Condition of Equivalence

In the previous section, we explain how ID and ZC distinguishers on a Feistel-type cipher can be found using a matrix method. However, the provided discussion shows that the matrices used in both context are different. While in the differential context the matrix $\mathcal{R}$ representing the round function can be used directly, in the linear context one should use the matrix $\mathcal{M}$ refereed as mirror matrix. Based on these remarks and on the fact that ZC distinguishers and ID distinguishers threaten usually the same number of rounds of many Feistel-type ciphers, we study in this section, the relation between these attacks. In particular we analyze the conditions which allow us to state that we have an ID distinguisher involving M differentials on $r = \ell + m$ rounds of the cipher if and only if we have a ZC distinguisher involving M linear approximations on the same $r = \ell + m$ rounds.

Theorem 1. *Let $\mathcal{R}$ be the matrix representation of the round function of a generalized Feistel Network as presented in Sect. 2 and $\mathcal{M}$ be the matrix representation of its mirror function. If it exists a $b \times b$ permutation matrix $\mathcal{Q}$ such that*

$$\mathcal{R} = \mathcal{Q} \cdot \mathcal{M} \cdot \mathcal{Q}^{-1} \text{ or } \mathcal{R} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}, \tag{1}$$

we deduce that:
It exists an impossible differential distinguisher on r rounds involving M differentials if and only if it exists a zero-correlation linear distinguisher on r rounds involving M linear masks.

Proof. As the second condition of (1) seems to be the most likely in practice, we assume in this proof that we have $\mathcal{R} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}$. The other case can be proved in a similar way.
We assume that we have an ID on $\ell + m$ rounds meaning that we know some Δ and Γ such that we have an inconsistency between $\mathcal{R}^{\ell} \cdot \Delta$ and $\mathcal{R}^{-m} \cdot \Gamma$.
As we have $\mathcal{R}^{\ell} = \mathcal{Q} \cdot \mathcal{M}^{-\ell} \cdot \mathcal{Q}^{-1}$ and $\mathcal{R}^{-m} = \mathcal{Q}^{-1} \cdot \mathcal{M}^{m} \cdot \mathcal{Q}$, we deduce that we have an inconsistency between $\mathcal{R}^{\ell} \cdot \Delta$ and $\mathcal{R}^{-m} \cdot \Gamma$, if and only if we have an inconsistency between $\mathcal{Q} \cdot \mathcal{M}^{-\ell} \cdot \mathcal{Q}^{-1} \cdot \Delta$ and $\mathcal{Q}^{-1} \cdot \mathcal{M}^{m} \cdot \mathcal{Q} \cdot \Gamma$. Given the masks $U = \mathcal{Q}^{-1} \cdot \Delta$ and $V = \mathcal{Q} \cdot \Gamma$, we deduce an inconsistency between $\mathcal{Q} \cdot \mathcal{M}^{-\ell} \cdot U$ and $\mathcal{Q}^{-1} \cdot \mathcal{M}^{m} \cdot V$.
Notice that the intermediate masks correspond to a linear permutation of the intermediate differences and that we have transformed the inconsistency in the differential context to an inconsistency in the linear context.

More precisely, we have shown that if it exists a permutation matrix Q such that $\mathcal{R} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}$, and if we have an ID distinguisher on $\ell + m$ rounds of a Feistel-type cipher, we have a ZC distinguisher on $m + \ell$ rounds of the same cipher. The converse proof is obtained by inverting the role played by $\mathcal{R}$ and $\mathcal{M}$. From the details provided in the proof, one can notice that since $\mathcal{Q}$ is a permutation matrix, the truncated masks and differences, U and Δ as well as V and Γ, are similar and the number of differences corresponds to the number of masks. □

Similarly one can prove that the linear and differential diffusion of a Feistel-type cipher are equal if the round function respect one of the conditions given in (1).

3.2 Example of Equivalence

In practice many Feistel-type ciphers respect the condition given in Th. 1. In this section, we discuss some of the well-known constructions.

For instance for the type-I Feistel-type cipher of Ex. 1 we have

$$\mathcal{Q} = \begin{pmatrix} 1\,0\,0\,0 \\ 0\,0\,0\,1 \\ 0\,0\,1\,0 \\ 0\,1\,0\,0 \end{pmatrix} \text{ and } \mathcal{R} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}.$$

Using this method, we can also show that any type-II Feistel-type ciphers have the same linear and differential diffusion.

The construction proposed by Nyberg [16] is, at the difference of the type-I and type-II one non-alternating, meaning that over the rounds the same branch can affected by many branching operations before being affected by a Xor. As this construction fulfills the condition given in Th 1, from the model proposed in this paper, one can easily adapt the security analysis provided against ID cryptanalysis to the linear context.

In [19], Suzaki and Minematsu proposed a general framework for all these Feistel-type ciphers. Based on this analysis, they later design the block cipher TWINE [21]. While the security of this cipher in regard to ID cryptanalysis has been analysed by the designers, up to our knowledge no analysis of the security/insecurity of this cipher in regard to ZC cryptanalysis has been done. In [20], the authors explain the similarity between TWINE and LBlock. From our framework, we can check that the 14-round ID distinguisher of LBlock or TWINE [21] can be converted directly to a 14-round zero-correlation one. As this distinguisher was considered in the security analysis performed by the designers and the round function of these ciphers fulfilled to conditions of Th. 1, one can question the relevance of, for instance, the zero-correlation attack of [18] on LBlock.

The next section is dedicated to the analysis of the results of [19].

3.3 Example of Non-Equivalence

In Appendix of [19], many Feistel-type round functions with different diffusion layers are proposed. Among other, the security in regards to ID cryptanalysis is analyzed for different permutations, π, of the 6, 8, 10, 12, 14 or 16 branches.

We checked the framework proposed in Th. 1 on these constructions. In particular, for each permutation π proposed in [19], using the matrix representation, we checked if it exists a permutation matrix $\mathcal{Q}$, such that one of the conditions given in (1) is satisfied. As no security analysis against zero-correlation linear attack is provided in [19], we compare our result (existence or non-existence of such matrix) with the differential and linear diffusion provided in [19]. While for most of them we can prove that the existence of an ID distinguisher implies the existence of a ZC distinguisher, for illustration purpose, we present here two cases where the condition given in Th. 1 is not satisfied. In Tables 1 and 2 both ciphers have an impossible distinguisher on 14 rounds and after 8 rounds 38, 40 or 35 Sboxes are active in the differential or linear context.

Table 1. Case No.12 of Table 5 of [19] ($b = 14$).

π	Number of rounds		Number of active Sboxes	
	impossible	diffusion	diff. context	linear context
$\{1, 2, 9, 4, 11, 6, 7, 8, 5, 12, 13, 10, 3, 0\}$	14	8	38	40

The permutation defined Table 1 is such that the minimal number of active Sboxes after 8 rounds in the differential context is smaller than the one in the linear context, this results is confirmed by the fact that we can prove that there exists no-matrix $\mathcal{Q}$ verifying the condition given in Th. 1. The diffusion (number

Table 2. Case No.5 of Table 4 of [19] ($b = 12$).

π	Number of rounds		Number of active Sboxes	
	impossible	diffusion	diff. context	linear context
$\{5, 0, 7, 2, 1, 6, 11, 8, 3, 10, 9, 4\}$	14	8	35	35

of active Sboxes) in the linear and differential context of the Feistel-type function given in Table 2 has been computed as equal. With the method described in this paper, we can show that the condition of Th. 1 is not fulfilled. This example illustrates the possibility that the conditions given in Th. 1 are sufficient but not necessary to have the same linear and differential diffusion.

4 Equivalence for Skipjack-Type Ciphers

4.1 Skipjack-Type Ciphers

Some word-oriented ciphers, which are also vulnerable to ID and ZC do not fulfill the conditions given in Sect. 3. This is for instance the case of the cipher Skipjack and its two different round functions known as Rule-A and Rule-B.

Fig. 3. Rule-A (left) and Rule-B (right) as in Skipjack

For these functions represented in Fig. 3, the internal non-linear functions should be bijective to allow the decryption.

In this section, a Skipjack-type cipher is defined as an iteration of Skipjack-type round functions. For such round function the input and output of a non-linear function are on the same branch. Such round function can have one non-linear bijective function in each of its branch. We assume that the linear operations consisting at mixing the information of the different branches are executed after the F-layer. We call this step X-layer. In this section, we assume that only one branching or exclusive-or operation is allowed on each branches. The permutation of the branches, P-layer, is the last operation performed in this round function. More precisely, using a matrix representation, a Skipjack-type round function can be described as follows.

Definition 3. *A Skipjack-type round function with b branches can be matricially represented as a combination of three $b \times b$ matrices $\mathcal{G}$, $\mathcal{X}$, $\mathcal{P}$ with coefficients $\{0, 1, F\}$, where F denotes a non-linear layer operation.*

- *Representing the F-layer, the matrix $\mathcal{G}$ is diagonal with 1 or F in the diagonal. The j-th element of the diagonal is equal to F if a non-linear function is applied to the branch j.*
- *Representing the X-layer, the matrix $\mathcal{X}$ has 1's in the diagonal and at maximum two 1 per row and column.*
- *Representing the P-layer, the matrix $\mathcal{P}$ is a permutation matrix with only one non-zero element per line and column.*

From these three matrices, a Skipjack-type round function can be represented by a $b \times b$ matrix $\mathcal{R}$ defined as $\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{G}$.

Example 3. Rule-A of Skipjack depicted in Fig. 3 can be represented as

$$\mathcal{R}_A = \mathcal{P} \cdot \mathcal{X}_A \cdot \mathcal{G} = \begin{pmatrix} F & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ F & 0 & 0 & 0 \end{pmatrix},$$

$$\text{with } \mathcal{X}_A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \mathcal{G} = \begin{pmatrix} F & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \mathcal{P} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Def. 3 covers more constructions than just the Rule-A of the Skipjack. In Fig. 4 an other example of Skipjack-type function with two non-linear functions and different P-layer is represented.

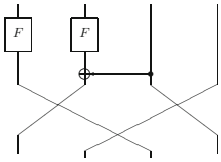


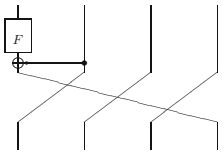
Fig. 4. A Skipjack-type round function with two internal non-linear layers

ID distinguishers can be found using this matrix representation. The inconsistency rules and the properties defined in Fig. 2 remains the same than for a Feistel-type cipher.

As in Sect. 3, we identify -1 as 1, $-F$ as F but also in this section, we identify $1/F$ and F^{-1} as F.

Definition 4. *Given $\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{G}$ the matrix representation of a Skipjack-type round function (see. Def. 3), we call mirror function the round function described by the matrix $\mathcal{M} = \mathcal{P} \cdot \mathcal{X}^T \cdot \mathcal{G}$.*

Example 4. The mirror of the Skipjack Rule-A round function given in Fig. 3 is:



$$\text{with } \mathcal{M} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ F & 1 & 0 & 0 \end{pmatrix}.$$

Similarly to the description provided in Sect. 2.3 for Feistel-type ciphers, this mirror representation can be use find ZC distinguishers on a cipher defined as an iteration of a unique Skipjack-type round function.

4.2 Condition of Equivalence

In this section, before describing in Th. 2 under which condition, the existence of an ID distinguisher involving M differences is equivalent to the existence of a ZC distinguisher involving M linear masks, we explain why the Rule-B of Skipjack depicted in Fig. 3, can be represented in our model.

Rule-B of Skipjack depicted in Fig. 3 can be represented using the matrices $\mathcal{G}$ and $\mathcal{P}$ of Ex. 3 as

$$\mathcal{R}_B = \mathcal{P} \cdot \mathcal{G} \cdot \mathcal{X}_B = \begin{pmatrix} F & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \text{ with } \mathcal{X}_B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Notice that for $\mathcal{R}_B$ at contrary to $\mathcal{R}_A$ the X-layer is performed before the F-layer. Nevertheless, when it comes at computing the differential and linear diffusion but also at finding ID or ZC distinguishers of a cipher defined as an iteration

of Rule-B, the first and or last linear layer can be omitted or interchanged. More explicitly we can define new round function with matrix representation: $\mathcal{R}_* = \mathcal{X}_B \cdot \mathcal{P} \cdot \mathcal{G} = \mathcal{P} \cdot (\mathcal{P}^{-1} \cdot \mathcal{X}_B \cdot \mathcal{P}) \cdot \mathcal{G}$. This transformed function corresponds to the mirror of Rule-A given in Ex. 4.

Remark 1. In a general matter, if the X-layer is performed before the F-layer, meaning if the round function is represented as $\mathcal{R} = \mathcal{P} \cdot \mathcal{G} \cdot \mathcal{X}$ with $\mathcal{P}, \mathcal{X}, \mathcal{G}$ as in Def. 3, for studying the differential and linear properties, we can transform of this round function to fulfill the Def. 3 of a Skipjack-type cipher. The matrix representation of this transformed round function can be computed as $\mathcal{R}_* = \mathcal{X} \cdot \mathcal{P} \cdot \mathcal{G} = \mathcal{P} \cdot (\mathcal{P}^{-1} \cdot \mathcal{X} \cdot \mathcal{P}) \cdot \mathcal{G}$.

While the number of differences (resp. masks) considered in an ID (resp. ZC) distinguisher remain the same for the transformed round function than for the original one, the input/output differences (resp. masks) pattern can be different for the transformed cipher than for the original one. For instance, as illustrated in Table 3, when iterating only Rule-B the input differences of the ID distinguisher are equal in two of the branches, while when iterating only Rule-A the input differences are non-zero in only one of the branches.

In this section we assume a cipher with identical round functions. Discussion for construction with different rules will be provided in Sect. 4.3.

Theorem 2. *Let $\mathcal{R}$ be the matrix representation of a Skipjack-type round function as in Def. 3 and $\mathcal{M}$ be its mirror function. If it exists a $b \times b$ permutation matrix $\mathcal{Q}$ such that*

$$\mathcal{R} = \mathcal{Q} \cdot \mathcal{M} \cdot \mathcal{Q}^{-1} \text{ or } \mathcal{G} \cdot \mathcal{P} \cdot \mathcal{X} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}, \tag{2}$$

we deduce that:
It exists an impossible differential distinguisher on r rounds involving M differentials if and only if it exists a zero-correlation linear distinguisher on r rounds involving M linear masks.

Proof. The proof is similar to the one of Th. 1. While the proof is easy for the first condition of (2), we assume here that $\mathcal{G} \cdot \mathcal{P} \cdot \mathcal{X} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}$. The different steps of the proof for the Rule-A of Skipjack are illustrated in Fig. 5.

From Def. 3, we have $\mathcal{R}^{-1} = \mathcal{G}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1}$ or equivalently $\mathcal{R}^{-1} = \mathcal{P}^{-1} \cdot (\mathcal{P} \cdot \mathcal{G}^{-1} \cdot \mathcal{P}^{-1}) \cdot (\mathcal{P} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1})$. One can notice that the order of the operations of the inverse of the round function does not match the order of the mirror function or even the one of the round function. From Rem. 1, we can modify the round function to obtain the transformed function $\mathcal{R}_*^{-1} = \mathcal{P} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1} \cdot \mathcal{G}^{-1} \cdot \mathcal{P}^{-1} = \mathcal{P} \cdot (\mathcal{R}_*)^{-1} \cdot \mathcal{P}^{-1}$.

We have an inconsistency between $\mathcal{R}^{\ell} \cdot \Delta$ and $\mathcal{R}^{-m} \cdot \Gamma$ if and only if we have an inconsistency between $\mathcal{R}_*^{\ell} \cdot \Delta_*$ and $\mathcal{R}_*^{-m} \cdot \Gamma_*$, where Δ_* and Γ_* are linear combinations of Δ and Γ and where $\mathcal{R}_* = (\mathcal{R}_*^{-1})^{-1}$. More explicitly, if and only if we have an inconsistency between $\left[\mathcal{P} \cdot (\mathcal{G} \cdot \mathcal{P} \cdot \mathcal{X})^l \cdot \mathcal{P}^{-1}\right] \cdot \Delta_*$ and $\left[\mathcal{P} \cdot (\mathcal{X}^{-1} \cdot \mathcal{P}^{-1} \cdot \mathcal{G}^{-1})^m \cdot \mathcal{P}^{-1}\right] \cdot \Gamma_*$.

Assuming representatives of the linear masks U and V similar to Δ_* and Γ_* this means that we have an inconsistency between $\left[\mathcal{P} \cdot (\mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1})^l \cdot \mathcal{P}^{-1}\right] \cdot V$ and $\left[\mathcal{P} \cdot (\mathcal{Q} \cdot \mathcal{M} \cdot \mathcal{Q}^{-1})^m \cdot \mathcal{P}^{-1}\right] \cdot U$.
And we deduce an inconsistency between $\mathcal{S} \cdot \mathcal{M}^{-\ell} \cdot \mathcal{S}^{-1} \cdot V$ and $\mathcal{S} \cdot \mathcal{M}^m \cdot \mathcal{S}^{-1} \cdot U$ where $\mathcal{S} = \mathcal{P} \cdot \mathcal{Q}$ is a permutation matrix. Meaning that we have transformed an ID distinguisher on $\ell + m$ rounds to a ZC distinguisher on $m + \ell$ rounds. □

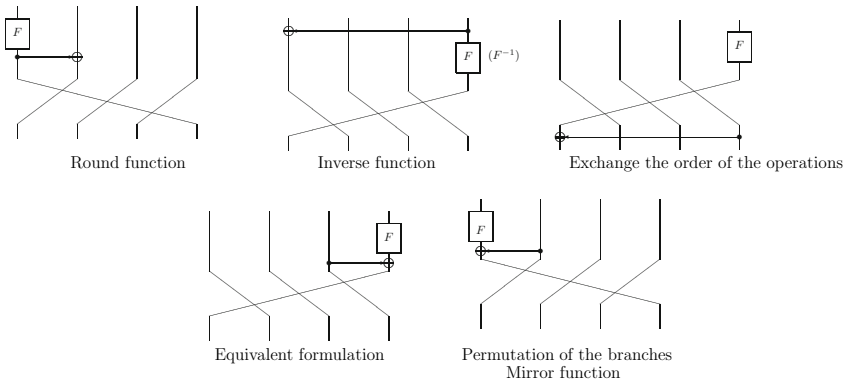


Fig. 5. Illustration of the different steps in the proof of Th. 2 for Rule-A of Skipjack

4.3 Example of Skipjack-Type Ciphers

While Skipjack is defined as a 32-round cipher where 8 rounds of Rule-A are followed by 8 rounds of Rule-B, analysis of different variants using different combination of these rules can be found in the literature. In this section, we discuss these different variants.

Taken independently, Rule-A and Rule-B fulfill the condition given in Th. 2 and a cipher using only one of these rules will have ZC and ID distinguishers on the same number of rounds.

But using a combination of theses rules, we know [7] that ZC and ID distinguishers are inequivalent (see Table 3). In particular, the number of rounds on which the distinguisher can be applied depends on the alternation. For instance the original Skipjack where 8 rounds of Rule-A are followed by 8 rounds of Rule-B is more resistant to ZC cryptanalysis than to ID cryptanalysis [7].

Table 3. ID and ZC for different variants of Skipjack

Structure	Impossible Differential		Zero-Correlation Linear Hull	
	rounds	pattern	rounds	pattern
Original	24	$(0,\delta,0,0) \nrightarrow (\gamma,0,0,0)$	17	$(u,0,0,0) \nrightarrow (v,v,0,0)$
(4 Rule-A, 4 Rule-B)	21	$(0,\delta,0,0) \nrightarrow (\gamma,0,0,0)$	30	$(u,u,0,0) \nrightarrow (v,v,0,0)$
(only Rule-A)	16	$(0,\delta,0,0) \nrightarrow (\gamma,\gamma,0,0)$	16	$(u,0,0,0) \nrightarrow (v,v,0,0)$
(only Rule-B)	16	$(\delta,\delta,0,0) \nrightarrow (\gamma,0,0,0)$	16	$(u,u,0,0) \nrightarrow (0,v,0,0)$

This example illustrates that when designing a cipher using a combination of different round functions, a more precise analysis than the one proposed in this paper may be required. Below we describe an analysis for a variant where a round with Rule-B is followed directly by a round with Rule-A.

After analysis we can show that when Rule-B is followed by Rule-A the two rounds are equivalent, in the sense of Rem. 1, to the round function given in Fig. 4. The matrix representation of this round function is:

$$\mathcal{R}_{BA} = \mathcal{P}_{BA} \cdot \mathcal{X}_{BA} \cdot \mathcal{G}_{BA} = \begin{pmatrix} 0 & F & 1 & 0 \\ 0 & 0 & 0 & 1 \\ F & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ with}$$

$$\mathcal{X}_{BA} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \mathcal{G}_{BA} = \begin{pmatrix} F & 0 & 0 & 0 \\ 0 & F & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \mathcal{P}_{BA} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

From simple computation, we can show that neither this function nor its inverse are equivalent to its mirror function. This observation can most probably explain why ID and ZC distinguishers can not be applied of the same numbers of rounds for different variants of Skipjack.

5 Other Constructions

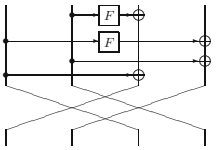
5.1 Generalized Feistel-Type Ciphers

For some constructions such as the one proposed by Berger, Minier, Thomas in [1], the round function can be decomposed into a non-linear layer, F-layer, similar to the one of Feistel-type cipher (see Sect. 2), a X-layer similar to the one described for the Skipjack-type cipher (see Sect. 4) and a permutation layer (P-layer). A full description of these layers can be found in [1]. An example with 4 branches of the construction proposed in [1] is depicted in Fig. 6.

In this section we denote by $\mathcal{F}, \mathcal{X}, \mathcal{P}$, the matrix representation of the different layers, where $\mathcal{F}$ and $\mathcal{P}$ are defined as in Def. 1, and $\mathcal{X}$ is defined as in Def. 3. The round function of the construction described in this section can be represented by the product of these three matrices $\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$.

For such constructions, one can see that ZC distinguishers can be found thanks to the matrix $\mathcal{M} = \mathcal{P} \cdot \mathcal{X}^T \cdot \mathcal{F}^T$, which corresponds to the representation of the mirror round function.

Similarly than for Th. 1 and 2 we derive conditions on the equivalence between ID and ZC distinguishers with same number of differences and masks.



$$\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F} \text{ with } \mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & F & 1 & 0 \\ F & 0 & 0 & 1 \end{pmatrix},$$

$$\mathcal{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \text{ and } \mathcal{P} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Fig. 6. Round function proposed in Fig. 3 of [1] and its matrix representation (Example with 4 branches)

Theorem 3. *Let $\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$ be the matrix representation of a generalized Feistel-type round function and $\mathcal{M} = \mathcal{P} \cdot \mathcal{X}^T \cdot \mathcal{F}^T$ be its mirror function. If it exists a permutation matrix Q such that*

$$\mathcal{R} = \mathcal{Q} \cdot \mathcal{M} \cdot \mathcal{Q}^{-1} \text{ or } \mathcal{R} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}, \text{ or } \mathcal{F} \cdot \mathcal{P} \cdot \mathcal{X} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}, \quad (3)$$

we deduce that:
It exists an impossible differential distinguisher on r rounds involving M differentials if and only if it exists a zero-correlation linear distinguisher on r rounds involving M linear masks.

The round functions of Sect. 2.2 of [1] fulfill the model presented in this section. In particular, one can check that $\mathcal{R} = \mathcal{M}^{-1}$. While in the original paper, the security in regard to ZC cryptanalysis is not measured, thanks to the analysis presented in this paper we are able to prove the existence of ZC distinguishers on the same number of rounds than the ID distinguishers.

5.2 Constructions Similar to MARS and Four-Cell

For some of the constructions depicted in Fig. 7, the output of the round function can in the same round influence many branches (i.e. MARS [15]) or many branches can be used to determine the input of a non-linear function (i.e. SMS4 [17]). While the round function of MARS can be represented using the following matrices,

$$\mathcal{R} = \mathcal{P} \cdot \mathcal{F} \text{ with } \mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ F & 1 & 0 & 0 \\ F & 0 & 1 & 0 \\ F & 0 & 0 & 1 \end{pmatrix} \text{ and } \mathcal{P} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

one can see that this decomposition does not correspond to the one of the round function of a Feistel-type cipher.

In [13], the authors show the existence of an ID distinguisher on 11 rounds on MARS: $(0,0,0,\delta) \nrightarrow (\delta,0,0,0)$, $\delta \in \mathbb{F}_2^s$, and the existence of a 11-round ID distinguisher on SMS4: $(\delta,\delta,\delta,0) \nrightarrow (0,\delta,\delta,\delta)$, $\delta \in \mathbb{F}_2^s$. As we can easily see from Fig. 7 that the round function of SMS4 is the mirror function of the

round function of MARS, we deduce directly a ZC distinguisher on 11 rounds of MARS: $(u, u, u, 0) \nrightarrow (0, u, u, u)$, $u \in \mathbb{F}_2^s$ as well as a 11-round ZC distinguisher on SMS4. Notice that for these two round functions we can easily see that it exists a permutation matrix $\mathcal{Q}$ such that $\mathcal{R}^{-1} = \mathcal{Q} \cdot \mathcal{R} \cdot \mathcal{Q}^{-1}$.

More generally, to perform a similar analysis on this construction than the analysis presented in Sect. 5.1, one can give a more precise decomposition of the matrix representation. For a better understanding, we illustrate in Fig. 7 this decomposition in the case of MARS and SMS4.

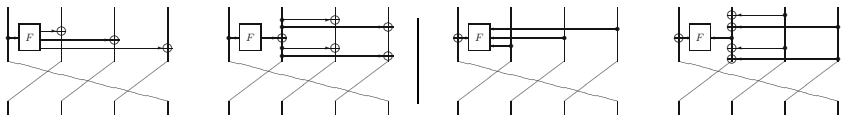


Fig. 7. Left: Round function of MARS and equivalent representation. Right: Round function of SMS4 and equivalent representation.

Let $\mathcal{Y}$ represent the first X-layer and be defined as the matrix $\mathcal{X}$ of Def. 3, a round function of a MARS-type cipher can be decomposed as $\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F} \cdot \mathcal{Y}$. Based on Rem. 1, we can analyze the transformed function: $\mathcal{R}_* = \mathcal{Y} \cdot \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F} = \mathcal{P} \cdot (\mathcal{P}^{-1} \cdot \mathcal{Y} \cdot \mathcal{P} \cdot \mathcal{X}) \cdot \mathcal{F}$. If we denote $\mathcal{X}'_* = \mathcal{P}^{-1} \cdot \mathcal{Y} \cdot \mathcal{P} \cdot \mathcal{X}$ we have $\mathcal{R}_* = \mathcal{P} \cdot \mathcal{X}'_* \cdot \mathcal{F}$.

For this type of construction where the X-layer is represented by a matrix $\mathcal{X}'$ similar to the matrix $\mathcal{X}$ of Def. 3 but where we can have more than two "1" per row or column, another arithmetic is required. In particular, one should assume that $F(\delta_1) \oplus F(\delta_2) = F(\delta_1 + \delta_2)$ meaning that F is linear when it comes to analyze the differential and linear properties of the cipher.

By noticing that this transformed round function corresponds to the description of the Generalized Feistel-type cipher of Sect. 5.1, one can verify that for both MARS and SMS4, none of the conditions described in (3) are satisfied.

In ASISP 2009 [10] a construction called GF-NLFSR was proposed. For this construction which is a generalization of the Skipjack-type construction, many operations on the branches can be performed in the same rounds. The four branches instance of this construction is known as Four-Cell.

Similarly than for ciphers of the previous type one can determine under which condition we can convert an ID distinguisher using M differences to a ZC distinguisher using M linear masks. This simple analysis show that the mirror round function of Four-Cell is not equivalent to the function or its function, and while the best known ID distinguisher is on 18 rounds [22], we were only able to find a ZC distinguisher on 12 rounds.

6 Conclusion

Understanding the relations between ID and ZC is of great importance to simplify the analysis by designers and cryptanalysts. In this paper, we show that for some constructions based on the generalizations of the well-known Feistel and Skipjack constructions, ZC distinguishers and ID distinguishers can be derived

from each other. In particular, we show that, if a round function and its mirror representation are related, both distinguishers cover the same number of rounds. Examples of ciphers for which we can prove such an equivalence are provided, along with a discussion of inequivalent cases. While we do not claim to have considered all types of word-oriented ciphers, this work is bridging the gap between these two attacks and allows for a better understanding of how to design ciphers with similar ID and ZC properties. The question of equivalence between corresponding key-recovery attacks – applied on top of those distinguishers – has been tackled in [5] and remains dependent on the outer rounds.

Acknowledgements. This work has been supported by the National Basic Research 973 Program of China under Grant No. 2013CB834205, National Natural Science Foundation of China under Grant No. 61133013, Program for New Century Excellent Talents in University of China under Grant No. NCET-13-0350, as well as the Interdisciplinary Research Foundation of Shandong University of China under Grant No. 2012JC018.

References

1. Berger, T.P., Minier, M., Thomas, G.: Extended Generalized Feistel Networks using Matrix Representation. In: SAC 2013 (to appear)
2. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999)
3. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991)
4. Blondeau, C., Nyberg, K.: New Links between Differential and Linear Cryptanalysis. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 388–404. Springer, Heidelberg (2013)
5. Blondeau, C., Nyberg, K.: Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. In: Oswald, E., Nguyen, P.Q. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 165–182. Springer, Heidelberg (2014)
6. Bogdanov, A., Geng, H., Wang, M., Wen, L., Collard, B.: Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. In: SAC 2013. LNCS. Springer (2014)
7. Bogdanov, A., Leander, G., Nyberg, K., Wang, M.: Integral and Multidimensional Linear Distinguishers with Correlation Zero. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 244–261. Springer, Heidelberg (2012)
8. Bogdanov, A., Rijmen, V.: Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Designs, Codes and Cryptography 70(3), 369–383 (2014)
9. Bogdanov, A., Wang, M.: Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 29–48. Springer, Heidelberg (2012)
10. Choy, J., Chew, G., Khoo, K., Yap, H.: Cryptographic Properties and Application of a Generalized Unbalanced Feistel Network Structure. In: Boyd, C., González Nieto, J. (eds.) ACISP 2009. LNCS, vol. 5594, pp. 73–89. Springer, Heidelberg (2009)

11. Kim, J., Hong, S., Lim, J.: Impossible differential cryptanalysis using matrix method. Discrete Mathematics 310(5), 988–1002 (2010)
12. Knudsen, L.R.: DEAL- A 128-bit Block-Cipher. NIST AES Proposal (1998)
13. Luo, Y., Lai, X., Wu, Z., Gong, G.: A unified method for finding impossible differentials of block cipher structures. Inf. Sci. 263, 211–220 (2014)
14. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
15. Moriai, S., Vaudenay, S.: On the pseudorandomness of Top-Level schemes of block ciphers. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 289–302. Springer, Heidelberg (2000)
16. Nyberg, K.: Generalized Feistel Networks. In: Kim, K.-c., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 91–104. Springer, Heidelberg (1996)
17. SMS4. Specication of SMS4, block cipher for WLAN products SMS4 (in Chinese)
18. Soleimany, H., Nyberg, K.: Zero-Correlation Linear Cryptanalysis of Reduced-Round LBlock. In: International Workshop on Coding and Cryptography, WCC 2013, pp. 329–343 (2013)
19. Suzaki, T., Minematsu, K.: Improving the Generalized Feistel. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 19–39. Springer, Heidelberg (2010)
20. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: A Lightweight, Versatile Block Cipher. In: Leander, G., Standaert, F.-X. (eds.) ECRYPT Workshop on Lightweight Cryptography (2011)
21. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: A Lightweight Block Cipher for Multiple Platforms. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 339–354. Springer, Heidelberg (2013)
22. Wu, W., Zhang, L., Zhang, L., Zhang, W.: Security analysis of the GF-NLFSR structure and Four-Cell block cipher. In: Qing, S., Mitchell, C.J., Wang, G. (eds.) ICICS 2009. LNCS, vol. 5927, pp. 17–31. Springer, Heidelberg (2009)
23. Wen, L., Wang, M., Bogdanov, A.: Multidimensional zero-correlation linear cryptanalysis of E2. In: Pointcheval, D., Vergnaud, D. (eds.) AFRICACRYPT 2014. LNCS, vol. 8469, pp. 147–164. Springer, Heidelberg (2014)
24. Wen, L., Wang, M., Bogdanov, A., Chena, H.: Multidimensional Zero-Correlation Attacks on Lightweight Block Cipher HIGHT: Improved Cryptanalysis of an ISO Standard. Information Processing Letters 114(6), 322–330 (2014)
25. Wu, S., Wang, M.: Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers. In: Galbraith, S., Nandi, M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 283–302. Springer, Heidelberg (2012)
26. Wu, W., Zhang, L.: LBlock: A Lightweight Block Cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344. Springer, Heidelberg (2011)