Provable Security Evaluation of Structures against Impossible Differential and Zero Correlation Linear Cryptanalysis ⋆

Bing Sun[1,2,4], Meicheng Liu[2,3], Jian Guo[2], Vincent Rijmen[5], Ruilin Li[6]

[1] College of Science, National University of Defense Technology, Changsha, Hunan, P.R.China, 410073
[2] Nanyang Technological University, Singapore
[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, P.R. China, 100093
[4] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, P.R. China, 100878
[5] Dept. Electrical Engineering (ESAT), KU Leuven and iMinds, Belgium
[6] College of Electronic Science and Engineering, National University of Defense Technology, Changsha, Hunan, P.R.China, 410073
happy_come@163.com meicheng.liu@gmail.com ntu.guo@gmail.com
vincent.rijmen@esat.kuleuven.be securitylrl@163.com

Abstract. Impossible differential and zero correlation linear cryptanalysis are two of the most important cryptanalytic vectors. To characterize the impossible differentials and zero correlation linear hulls which are independent of the choices of the non-linear components, Sun *et al.* proposed the structure deduced by a block cipher at CRYPTO 2015. Based on that, we concentrate in this paper on the security of the SPN structure and Feistel structure with SP-type round functions. Firstly, we prove that for an SPN structure, if $\alpha_1 \rightarrow \beta_1$ and $\alpha_2 \rightarrow \beta_2$ are possible differentials, $\alpha_1|\alpha_2 \rightarrow \beta_1|\beta_2$ is also a possible differential, i.e., the OR "|" operation preserves differentials. Secondly, we show that for an SPN structure, there exists an r-round impossible differential if and only if there exists an r-round impossible differential $\alpha \not\rightarrow \beta$ where the Hamming weights of both α and β are 1. Thus for an SPN structure operating on m bytes, the computation complexity for deciding whether there exists an impossible differential can be reduced from $\mathcal{O}(2^{2m})$ to $\mathcal{O}(m^2)$. Thirdly, we associate a primitive index with the linear layers of SPN structures. Based on the matrices theory over integer rings, we prove that the length of impossible differentials of an SPN structure is upper bounded by the primitive index of the linear layers. As a result we show that, unless the details of the S-boxes are considered, there do

⋆ The work in this paper is supported by the National Natural Science Foundation of China(No: 61303258, 61379139, 61402515, 61572026, 11526215), National Basic Research Program of China (973 Program) (2013CB338002), the Strategic Priority Research Program of the Chinese Academy of Science under Grant No. XDA06010701 and the Research Fund KU Leuven, OT/13/071. Part of the work was done while the first author was visiting Nanyang Technological University in Singapore.

not exist 5-round impossible differentials for the AES and ARIA. Lastly, based on the links between impossible differential and zero correlation linear hull, we projected these results on impossible differentials to zero correlation linear hulls. It is interesting to note some of our results also apply to the Feistel structures with SP-type round functions.
Key words: Impossible differential, Zero correlation linear, SPN structure, Feistel structure, AES, Camellia, ARIA

1 Introduction

Block ciphers are the vital elements in constructing many symmetric cryptographic schemes and the core security of these schemes depends on the resistance of the underlying block ciphers to known cryptanalytic techniques. Differential cryptanalysis [4] and linear cryptanalysis [20] are among the most famous cryptanalytic tools. Nowadays, most block ciphers are designed to be resilient to these two attacks. To prove the security of a block cipher against differential/linear attack, a common way is to give an upper bound on the rounds of the differential characteristics/linear trails that can distinguish a round-reduced cipher from a random permutation. Or equivalently, one can show when the number of the rounds of a block cipher is more than a certain r, there do not exist any useful differential characteristics or linear trails. However, the security margin of the ciphers against extended differential and linear cryptanalysis, such as impossible differential [3, 13] and zero correlation linear cryptanalysis [6], may not be yet well studied and formulated. To some extend, the success of such attacks relies mainly on the attackers' intensive analysis of the structures used in each individual designs.

In differential cryptanalysis, one usually finds differential characteristics with high probability and then uses statistical methods to sieve the right keys. However, the main idea of impossible differential cryptanalysis, which was independently proposed by Knudsen [13] and Biham *et al.* [3], is to use differentials that hold with probability zero to discard the wrong keys. So far, impossible differential cryptanalysis has received lots of attention and been used to attack a variety of well-known block ciphers [5, 7, 16, 22].

The first step in impossible differential cryptanalysis is to construct some impossible differentials that cover as many rounds as possible. For any function $F : \mathbb{F}_{2^b} \to \mathbb{F}_{2^b}$, we can always find some α and β such that $\alpha \to \beta$ is an impossible differential of F. However, when b is large and we know little about the algebraic structure of F, it is hard to determine whether $\alpha \to \beta$ is a possible differential or an impossible one. A block cipher $E(\cdot, k)$ may exhibit a differential $\alpha \to \beta$ that is a possible differential for some key k while it is impossible for the rest. In practice, such differentials are difficult to determine in most of the cases. Generally, in a search for impossible differentials it is difficult to guarantee completeness. Therefore, from the practical point of view, we are more interested in the impossible differentials that are independent of the secret keys. Since in most cases the non-linear transformations applied to x can be written as $S(x \oplus k)$, we always employ impossible differentials that are independent

of the S-boxes, which are called *truncated impossible differentials*, i.e., we only detect whether there are differences on some bytes and we do not care about the values of the differences. Usually, an impossible differential is constructed by the miss-in-the-middle technique, i.e., trace the properties of input and output differences from the encryption and decryption directions, respectively, if there are some contradictions in the middle, an impossible differential is then found. Several automatic approaches have been proposed to derive truncated impossible differentials of a block cipher effectively such as the $\mathcal{U}$-method [12], *UID*-method [18] and the extended tool of the former two methods generalized by Wu and Wang [24] (WW-method). It has been proved in [21] that the WW-method can find all impossible differentials of a structure, or equivalently, it can find all impossible differentials of a block cipher which are independent of the choices of the non-linear components. Similar ideas have found applications in cryptanalysis against hash functions BMW [10] and BLAKE [2].

In linear cryptanalysis, one uses linear characteristics with high correlations. Zero correlation cryptanalysis is a novel technique for cryptanalysis of block ciphers [6]. The distinguishing property used in zero correlation cryptanalysis is the zero correlation linear approximations, i.e., those linear approximations that hold with a probability $p = 1/2$, that is, strictly unbiased approximations having a correlation $c = 2p - 1$ equal to 0. As in impossible differential cryptanalysis, we are more interested in the zero correlation linear hulls that are independent of the choices of the non-linear layers.

In CRYPTO 2015, Sun *et al.* proposed the concept of *structure* to characterize what "being independent of the choices of the S-boxes" means, and proposed *dual structure* to study the link between impossible differentials and zero correlation linear hulls [21]. One of the basic statements in [21] is that constructing impossible differentials of a structure is equivalent to constructing zero correlation linear hulls of the dual structure. Therefore, all the known methods to construct impossible differentials of structures can also be used to construct zero correlation linear hulls.

Despite the known 4-/4-/8-round impossible differentials for the AES, ARIA and Camellia without FL/FL^{-1} layers [1, 9, 14, 17, 19, 25], effort to find new impossible differentials of these ciphers that cover more rounds has never stopped. On the other hand, we already have some novel techniques such as the wide trail strategy [8] and the decorrelation theory [23] to prove that a cipher is resilient to differential and linear attacks. However, the provable security of block ciphers against impossible differential and zero correlation linear cryptanalysis is still missing. Noting that for a dedicated iterated block cipher, there always exist impossible differentials for any rounds with some keys, we wonder that if we consider the impossible differentials that are independent of the choices of the S-boxes, there may exist an integer R such that there does not exist any impossible differentials that cover more than R rounds, which can give some insights on provable security of block ciphers against impossible differential and zero correlation linear cryptanalysis, i.e., R is the upper bound of such attacks. Furthermore, since the WW-method can only determine whether a given dif-

ferential/mask is an impossible differential/zero correlation linear hull or not, though it can theoretically find all impossible differentials/zero correlation linear hulls of a structure, it is impractical to exhaust all the differentials/masks to determine whether there exist r-round impossible differentials/zero correlation linear hulls or not. Therefore, finding new techniques to solve these problems in a practical way remains as an open problem.

Our Contributions. Inspired by the provable security of differential and linear cryptanalysis, this paper mainly concentrates on the provable security of block ciphers against impossible differential/zero correlation linear cryptanalysis and we aim at determining an upper bound for the longest rounds of impossible differentials/zero correlation linear hulls of SPN structures and Feistel structures with SPN round functions. The main results of this paper are as follows:

(1) For SPN structures, we prove that if $\alpha_1 \to \beta_1$ and $\alpha_2 \to \beta_2$ are possible differentials, then $\alpha_1|\alpha_2 \to \beta_1|\beta_2$ is also a possible differential, based on which we conclude that there exists an r-round impossible differential if and only if there exists an impossible differential $\alpha \to \beta$ where the Hamming weight of both α and β is 1. Therefore, for an SPN structure with m bytes, the complexity of testing whether there exist r-round impossible differentials is reduced significantly from $\mathcal{O}(2^{2m})$ to $\mathcal{O}(m^2)$.
(2) For Feistel structures with SP-type round functions, we prove that if $\alpha_1 \to \beta_1$ and $\alpha_2 \to \beta_2$ are *independent possible differentials* (we will define it later), then $\alpha_1|\alpha_2 \to \beta_1|\beta_2$ is also an independent possible differential, then similar result as in (1) applies.
(3) For any matrix over finite fields, we can always define two polynomials to calculate an upper bound on the highest possible rounds of impossible differentials of SPN structures and independent impossible differentials of Feistel structures with SP-type round functions. Our results show that, unless we take the details of the S-boxes into consideration, there do not exist 5-round impossible differentials of the AES and ARIA, and 9-round independent impossible differentials of Camellia without FL/FL^{-1} layers.
(4) Since the zero correlation linear hull of a structure is equivalent to the impossible differential of its dual structure, our results on impossible differentials cryptanalysis also apply to zero correlation linear cryptanalysis.

From the theoretical point of view, our results demonstrate some direct insight to the longest possible rounds of truncated impossible differentials and zero correlation linear hulls. And from the practical point of view, our results could reduce the work effort to find impossible differentials and zero correlation linear hulls of a structure.

Organization. The rest of this paper is organized as follows. Section 2 will introduce some definitions that will be used throughout this paper. In Section 3, we give some new features of the structures. We investigate on the SPN structures and Feistel structures with SP-type round functions in Section 4 and Section 5, respectively. Section 6 concludes the paper.

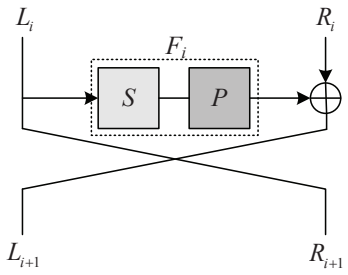

Fig. 1. Feistel structure with SP-type round functions

2 Preliminaries

2.1 Block Ciphers

SPN Ciphers. The SPN structure is widely used in constructing cryptographic primitives. It iterates some SP-type round functions to achieve confusion and diffusion. Specifically, the SP-type function $f : \mathbb{F}_{2^b}^m \to \mathbb{F}_{2^b}^m$ used in this paper is defined as follows.

Assume the input x is divided into m pieces $x = (x_0, \ldots, x_{m-1})$, where x_i is a b-bit byte. First, apply the non-linear transformation s_i to x_i,

$$y = S(x) \triangleq (s_0(x_0), \ldots, s_{m-1}(x_{m-1})) \in \mathbb{F}_{2^b}^m.$$

Then, apply a linear transformation $P : \mathbb{F}_{2^b}^m \to \mathbb{F}_{2^b}^m$ to y, and Py is the output of f. Notice that the linear transformation in the last round of an r-round SPN structure is omitted, i.e., an r-round SPN cipher is simply denoted as $(SP)^{r-1}S$.

Feistel Ciphers. An r-round Feistel cipher E is defined as follows: Let $(L_0, R_0) \in \mathbb{F}_2^{2m}$ be the input of E. Iterate the following transformation r times:

$$\begin{cases} L_{i+1} = F_i(L_i) \oplus R_i \\ R_{i+1} = L_i \end{cases} \quad 0 \le i \le r-1,$$

where $L_i, R_i \in \mathbb{F}_2^m$, see Fig.1. The output of E is defined as the output of the r-th iteration. In this paper, we will focus on the case that F_i's are defined as SP-type functions.

2.2 Vectors and Matrices

Assume $\alpha, \beta \in \mathbb{F}_{2^b}^m$, where $\mathbb{F}_{2^b}^m$ is the vector space over $\mathbb{F}_{2^b}$ with dimension m. Then $\alpha|\beta$ is defined as the bit-wise `OR` operation of α and β. Let $\theta : \mathbb{F}_{2^b} \to \mathbb{F}_2$ be defined as

$$\theta(x) = \begin{cases} 0 & x = 0, \\ 1 & x \neq 0. \end{cases}$$

Then, for $X = (x_0, \ldots, x_{m-1}) \in \mathbb{F}_{2^b}^m$, the *truncated characteristic* of X is defined as

$$\chi(X) \triangleq (\theta(x_0), \ldots, \theta(x_{m-1})) \in \mathbb{F}_2^m.$$

The *Hamming weight* of X is defined as the number of non-zero elements of the vector, i.e. $H(X) = \#\{i | x_i \neq 0, i = 0, 1, \ldots, m-1\}$.

For $P = (p_{ij}) \in \mathbb{F}_{2^b}^{m \times m}$, denote by $\mathbb{Z}$ the integer ring, the *characteristic matrix* of P is defined as $P^* = (p_{ij}^*) \in \mathbb{Z}^{m \times m}$, where $p_{ij}^* = 0$ if $p_{ij} = 0$ and $p_{ij}^* = 1$ otherwise. A matrix $M \in \mathbb{Z}^{m \times m}$ is *non-negative* if all elements of M are non-negative, and *positive* if all elements of M are positive. Therefore, the characteristic matrix is always non-negative.

Definition 1. *Let $P \in \mathbb{F}_{2^b}^{m \times m}$, P^* be the characteristic matrix of P, and*

$$f_t(x) = x^t,$$
$$g_t(x) = \begin{cases} \sum_{i=0}^{h} x^{2i} & t = 2h, \\ \sum_{i=1}^{h} x^{2i-1} & t = 2h-1. \end{cases}$$

Then the minimal integer t such that $f_t(P^*)$ is a positive matrix is called type 1 primitive index of P, and the minimal integer t such that $g_t(P^*)$ is positive is called type 2 primitive index of P.

If the input X to the linear layer P is viewed as a column vector, then the output Y can also be viewed as a column vector which is computed as $Y = PX$. According to the definition of characteristic matrix, $p_{ij}^* = 0$ means the i-th output byte of the first round is independent of the j-th input byte. Generally, let $f_t(P^*) = (P^*)^t = (q_{ij})$, then $q_{ij} = 0$ means the i-th output byte of the t-round SPN cipher is independent of the j-th input byte. Furthermore, let $(P^*)^{t_1} + (P^*)^{t_2} = (u_{ij})$, then $u_{ij} = 0$ means the i-th output bytes of both the t_1-round and t_2-round SPN cipher are independent of j-th input byte. Similarly, let $g_t(P^*) = (w_{ij})$, then $w_{ij} = 0$ means the i-th output byte of the t-round Feistel cipher is independent of the j-th input byte.

2.3 Impossible Differentials and Zero Correlation Linear Hulls

Given a function $G : \mathbb{F}_2^n \to \mathbb{F}_2$, the correlation c of G is defined by

$$c(G(x)) \triangleq \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{G(x)}.$$

Given a function $G : \mathbb{F}_2^n \to \mathbb{F}_2^k$, the correlation c of the linear approximation for a k-bit output mask b and an n-bit input mask a is defined by

$$c(ax \oplus bG(x)) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{ax \oplus bG(x)}.$$

If $c(ax \oplus bG(x)) = 0$, then $(a \to b)$ is called a zero correlation linear hull of G. This definition can be extended as follows: let $A \subseteq \mathbb{F}_2^n$, $B \subseteq \mathbb{F}_2^k$, if for all $a \in A$ and $b \in B$, $c(ax \oplus bG(x)) = 0$, then $(A \to B)$ is also called a zero correlation linear hull of G.

Let $\delta \in \mathbb{F}_2^n$ and $\Delta \in \mathbb{F}_2^k$. The differential probability of $\delta \to \Delta$ is defined as

$$p(\delta \to \Delta) \triangleq \frac{\#\{x \in \mathbb{F}_2^n | G(x) \oplus G(x \oplus \delta) = \Delta\}}{2^n}.$$

If $p(\delta \to \Delta) = 0$, then $\delta \to \Delta$ is called an *impossible differential* of G, this definition follows that in [13, 3]. Let $A \subseteq \mathbb{F}_2^n$, $B \subseteq \mathbb{F}_2^k$. If for all $a \in A$ and $b \in B$, $p(a \to b) = 0$, $A \to B$ is called an *impossible differential* of G.

3 Differential Properties of Structures

In many cases, when constructing impossible differentials and zero correlation linear hulls, we are only interested in detecting whether there is a difference (mask) in an S-box or not, regardless of the actual value of the difference (mask) which leads to the following definition:

Definition 2 ([21]). *Let $E : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher with bijective S-boxes as the basic non-linear components.*

(1) *A* structure $\mathcal{E}^E$ *on $\mathbb{F}_2^n$ is defined as a set of block ciphers E' which is exactly the same as E except that the S-boxes can take all possible bijective transformations on the corresponding domains.*
(2) *Let $\alpha, \beta \in \mathbb{F}_2^n$. If for any $E' \in \mathcal{E}^E$, $\alpha \not\to \beta$ is an impossible differential (zero correlation linear hull) of E', $\alpha \not\to \beta$ is called an impossible differential (zero correlation linear hull) of $\mathcal{E}^E$.*

Thus the structure deduced by a single S layer can be written as $\mathcal{E}^S$; the structure deduced by a single S layer followed by a P layer can be written as $\mathcal{E}^{SP}$. If $\alpha \to \beta$ is not an impossible differential of $\mathcal{E}^E$, i.e., there exist some x and $E' \in \mathcal{E}^E$ such that $E'(x) \oplus E'(x \oplus \alpha) = \beta$, we call it a *possible differential* of $\mathcal{E}^E$.

Definition 3. *Let $\mathcal{E}$ be a structure and $\alpha \not\to \beta$ an impossible differential of $\mathcal{E}$. If for all α^* and β^* satisfying $\chi(\alpha^*) = \chi(\alpha)$ and $\chi(\beta^*) = \chi(\beta)$, $\alpha^* \not\to \beta^*$ are impossible differentials, we call $\alpha \not\to \beta$ an* independent impossible differential *of $\mathcal{E}$. Otherwise, we call it a* dependent impossible differential *of $\mathcal{E}$.*

As shown in [25], for any $\alpha \neq 0$ and $\beta \neq 0$,

$$(0|0|0|0|0|0|0|0, \alpha|0|0|0|0|0|0|0) \not\to (\beta|0|0|0|0|0|0|0, 0|0|0|0|0|0|0|0)$$

is an 8-round impossible differential of Camellia without FL/FL^{-1} layers. According to the definition, such an impossible differential is an independent impossible differential of Camellia without FL/FL^{-1} layers.

A dependent impossible differential means that there are some constraints on actual differences of both the input and output bytes. For example, for any given α, $(0,\alpha) \not\to (0,\alpha)$ is a 5-round impossible differential of Feistel structures with bijective round functions. However, we cannot determine that $(0,\alpha) \not\to (0,\beta)$ is an impossible differential for any $\alpha \neq \beta$. Thus, $(0,\alpha) \not\to (0,\alpha)$ is a dependent impossible differential of 5-round Feistel structure with bijective round functions.

Usually, we have many different ways to define a linear transformation, which means we have many different ways to express the matrix of the linear transformation. However, no matter which one we use, the transformation is always linear over $\mathbb{F}_2$, thus the bit-wise matrix representation of a linear transformation is call the *primitive representation*. The definition of dual structure is proposed to study the link between impossible differential and zero correlation linear hulls:

Definition 4 ([21]). *Let $\mathcal{F}_{SP}$ be a* Feistel structure *with SP-type round function, and let the primitive representation of the linear transformation be P. Let σ be the operation that exchanges the left and right halves of a state. Then the* dual structure *$\mathcal{F}_{SP}^{\perp}$ of $\mathcal{F}_{SP}$ is defined as $\sigma \circ \mathcal{F}_{P^TS} \circ \sigma$.*

Let $\mathcal{E}_{SP}$ be an SPN structure *with primitive representation of the linear transformation being P. Then the* dual structure *$\mathcal{E}_{SP}^{\perp}$ of $\mathcal{E}_{SP}$ is defined as $\mathcal{E}_{S(P^{-1})^T}$.*

Next, we are going to give some statements on the differential properties of structures while they may not hold for dedicated block ciphers.

Let $\mathcal{E}^{(r)}$ be an r-round iterated structure. If $\alpha \to \beta$ is a possible differential of $\mathcal{E}^{(r_1)}$, then for any x, there always exists $E_1 \in \mathcal{E}^{(r_1)}$ such that $E_1(x) \oplus E_1(x \oplus \alpha) = \beta$. If $\beta \to \gamma$ is a possible differential of $\mathcal{E}^{(r_2)}$, for $y = E_2(x)$, there always exists $E_2 \in \mathcal{E}^{(r_2)}$ such that $E_2(y) \oplus E_2(y \oplus \beta) = \gamma$. Let $E = E_2 \circ E_1$, we have $E(x) \oplus E(x \oplus \alpha) = \gamma$ which means $\alpha \to \gamma$ is a possible differential $\mathcal{E}^{(r_1+r_2)}$. See (1) for the procedures. Accordingly, for a structure $\mathcal{E}$, if there do not exist r-round impossible differentials, there do not exist R-round impossible differentials for any $R \geq r$.

$$E: \quad \begin{array}{ccccc} x & \xrightarrow{E_1} & y & \xrightarrow{E_2} & z \\ | & & | & & | \\ x \oplus \alpha & \xrightarrow{E_1} & y \oplus \beta & \xrightarrow{E_2} & z \oplus \gamma \end{array} \tag{1}$$

Next we show that $\alpha \to \beta$ is a possible differential of a single S layer $\mathcal{E}^S$ if and only if $\chi(\alpha) = \chi(\beta)$. Firstly, we cannot construct a bijective S-box such that a zero difference causes a non-zero difference. Secondly, let $\alpha = (\alpha_0, \ldots, \alpha_{m-1}), \beta = (\beta_0, \ldots, \beta_{m-1}) \in \mathbb{F}_{2^b}^m$. If $\chi(\alpha) = \chi(\beta)$, for any $x = (x_0, \ldots, x_{m-1}) \in \mathbb{F}_{2^b}^m$, we can always construct an $S = (s_0, \ldots, s_{m-1})$ where $s_i : \mathbb{F}_{2^b} \to \mathbb{F}_{2^b}$, such that $S(x) \oplus S(x \oplus \alpha) = \beta$, i.e., $s_i(x_i) \oplus s_i(x_i \oplus \alpha_i) = \beta_i$, $i = 0, \ldots, m-1$.

4 Cryptanalysis of SPN Structures

In this section, we will simply use $\mathcal{E}_{SP}^{(r)}$ to denote an r-round SPN structure.

4.1 How to Check Whether A Differential Is Impossible or Not

Assume $\alpha \to \beta$ is a possible differential of $\mathcal{E}_{SP}^{(r)}$. Then, there always exist some α' and β' such that

$$\alpha \xrightarrow{\mathcal{E}^S} \alpha' \xrightarrow{\mathcal{E}^{PS\cdots SP}} \beta' \xrightarrow{\mathcal{E}^S} \beta$$

is a possible differential of $\mathcal{E}_{SP}^{(r)}$. Thus for any α^* and β^* such that $\chi(\alpha^*) = \chi(\alpha)$, $\chi(\beta^*) = \chi(\beta)$,

$$\alpha^* \xrightarrow{\mathcal{E}^S} \alpha' \xrightarrow{\mathcal{E}^{PS\cdots SP}} \beta' \xrightarrow{\mathcal{E}^S} \beta^*$$

is still a possible differential. In other words, impossible differentials of SPN structures are independent impossible differentials.

Therefore, for an SPN structure, to check whether there exists an r-round impossible differential or not, one needs to test $(2^m - 1) \times (2^m - 1) \approx 2^{2m}$ candidates. However, this complexity could be further reduced as illustrated in the following.

Lemma 1. *Assume $m \leq 2^{b-1} - 1$. If $\alpha_1 \to \beta_1$ and $\alpha_2 \to \beta_2$ are possible differentials of $\mathcal{E}^{SP}$, then there always exist α and β such that*

$$\begin{cases} \chi(\alpha) = \chi(\alpha_1)|\chi(\alpha_2), \\ \chi(\beta) = \chi(\beta_1)|\chi(\beta_2), \end{cases}$$

and $\alpha \to \beta$ is a possible differential of $\mathcal{E}^{SP}$.

The proof of this lemma is shown in Appendix A. In the following, we always assume $m \leq 2^{b-1} - 1$ which fits well with most cases. Furthermore, since the last round only has the S layer, we have:

Corollary 1. *If $\alpha_1 \to \beta_1$ and $\alpha_2 \to \beta_2$ are possible differentials of $\mathcal{E}_{SP}^{(r)}$, $\alpha_1|\alpha_2 \to \beta_1|\beta_2$ is also a possible differential of $\mathcal{E}_{SP}^{(r)}$.*

Assume $(x_0, 0, \ldots, 0) \to (y_0, 0, \ldots, 0)$ and $(0, x_1, 0, \ldots, 0) \to (0, y_1, 0, \ldots, 0)$ are possible differentials of $\mathcal{E}_{SP}$, where x_0, x_1, y_0, y_1 are non-zero. Then according to Corollary 1, $(x_0, x_1, 0, \ldots, 0) \to (y_0, y_1, 0, \ldots, 0)$ is a possible differential. In other words, if $(x_0, x_1, 0, \ldots, 0) \to (y_0, y_1, 0, \ldots, 0)$ is an impossible differential of $\mathcal{E}_{SP}$, either $(x_0, 0, \ldots, 0) \to (y_0, 0, \ldots, 0)$ or $(0, x_1, 0, \ldots, 0) \to (0, y_1, 0, \ldots, 0)$ is an impossible differential. Generally, we have the following theorem:

Theorem 1. *There exists an impossible differential of $\mathcal{E}_{SP}^{(r)}$ if and only if there exists an impossible differential $\alpha \not\to \beta$ of $\mathcal{E}_{SP}^{(r)}$, where $H(\alpha) = H(\beta) = 1$, with $H(x)$ denoting the Hamming weight of x.*

Thus with the help of Theorem 1, for every SPN structure, and any (α, β) where $H(\alpha) = H(\beta) = 1$, we can use the WW-method to check whether $\alpha \to \beta$ is a possible differential or not. Therefore, we could reduce the complexities of checking whether there exists an impossible differential of an SPN structure from $\mathcal{O}(2^{2m})$ to $\mathcal{O}(m^2)$.

Since the zero correlation linear hull of $\mathcal{E}_{SP}$ is the impossible differential of $\mathcal{E}_{S(P^{-1})^T}$ which is also an SPN structure, we have the following:

Corollary 2. *There exists a zero correlation linear hull of* $\mathcal{E}_{SP}^{(r)}$ *if and only if there exists a zero correlation linear hull* $\alpha \not\to \beta$ *of* $\mathcal{E}_{SP}^{(r)}$ *where* $H(\alpha) = H(\beta) = 1$.

4.2 An Upper Bound for the Rounds of Impossible Differentials

As discussed above, we can use the WW-method to determine the maximal length of impossible differentials for an SPN structure. In the following, we are going to show an upper bound for the length of impossible differentials for an SPN structure, which only uses the property of the P layer. To characterize the longest impossible differential of an SPN cipher, we first recall that if $\beta = P\alpha$, then there always exist α_0 and β_0 such that $\chi(\alpha_0) = \chi(\alpha)$, $\chi(\beta_0) = \chi(\beta)$ and $\alpha_0 \to \beta_0$ is a possible differential of a single round of SPN structure. Then according to Corollary 1, the following theorem holds.

Theorem 2. *Let* $R_1(P)$ *and* $R_{-1}(P)$ *be the type* 1 *primitive indexes of* P *and* P^{-1} *respectively. Then there does not exist any impossible differential or zero correlation linear hull of* $\mathcal{E}_{SP}^{(r)}$ *for* $r \geq R_1(P) + R_{-1}(P) + 1$.

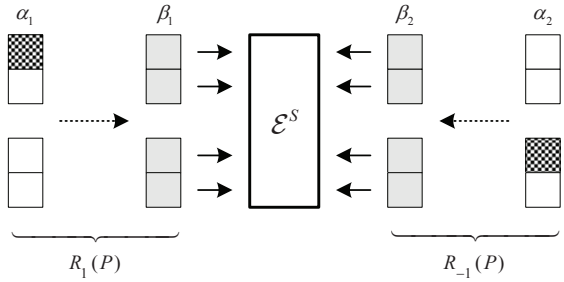

Fig. 2. Constructing $(R_1(P) + R_{-1}(P) + 1)$-round differential for $\mathcal{E}_{SP}$

Proof. See Fig.2. Firstly, for any $\alpha_1 \neq 0$, $H(\alpha_1) = 1$, according to Lemma 1, there always exist some β_1 where $H(\beta_1) = m$ such that $\alpha_1 \to \beta_1$ is a possible differential of $R_1(P)$-round $\mathcal{E}_{SP}$. Secondly, for any $\alpha_2 \neq 0$, $H(\alpha_2) = 1$, according to Lemma 1, there always exist some β_2 where $H(\beta_2) = m$ such that $\alpha_2 \to \beta_2$ is a possible differential of $R_{-1}(P)$-round decryption of $\mathcal{E}_{SP}$.

Since $\chi(\beta_1) = \chi(\beta_2)$, $\beta_1 \to \beta_2$ is a possible differential of the single S layer $\mathcal{E}^S$, we conclude that $\alpha_1 \to \alpha_2$ is a possible differential of $(R_1(P) + R_{-1}(P) + 1)$-round $\mathcal{E}_{SP}$. By Theorem 1, there does not exist any impossible differential or zero correlation linear hull of $\mathcal{E}_{SP}^{(r)}$ for $r \geq R_1(P) + R_{-1}(P) + 1$. □

4.3 Applications

The Advanced Encryption Standard (AES) is one of the most popular SPN ciphers up to date. Firstly, if we consider the 4×4 state as a vector in $\mathbb{F}_{2^8}^{16}$, the

composition of the ShiftRows and MixColumns can be written as the following 16×16 matrix over $\mathbb{F}_{2^8}$:

$$P = \begin{pmatrix}
2&0&0&0&0&3&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&2&0&0&0&0&3&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&2&0&0&0&0&3\\
3&0&0&0&0&1&0&0&0&0&1&0&0&0&0&2\\
0&0&0&1&2&0&0&0&0&3&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&2&0&0&0&0&3&0\\
0&0&0&3&1&0&0&0&0&1&0&0&0&0&2&0\\
0&0&0&2&3&0&0&0&0&1&0&0&0&0&1&0\\
0&0&1&0&0&0&0&1&2&0&0&0&0&3&0&0\\
0&0&3&0&0&0&0&1&1&0&0&0&0&2&0&0\\
0&0&2&0&0&0&0&3&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&2&3&0&0&0&0&1&0&0\\
0&3&0&0&0&0&1&0&0&0&0&1&2&0&0&0\\
0&2&0&0&0&0&3&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&2&0&0&0&0&3&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&2&3&0&0&0
\end{pmatrix}.$$

Therefore, the characteristic matrix of P is

$$P^* = \begin{pmatrix}
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0
\end{pmatrix}.$$

Since

$$(P^*)^2 = \begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix},$$

we get $R_1(P) = 2$. Similarly, we can get $R_{-1}(P) = 2$. Therefore, we have

Proposition 1. *There does not exist any impossible differential or zero correlation linear hull of $\mathcal{E}^{AES}$ which covers $r \geq 5$ rounds. Or equivalently, there does not exist any 5-round impossible differential or zero correlation linear hull of the AES unless the details of the S-boxes are considered.*

ARIA is another famous SPN cipher which uses a linear transformation P such that $P = P^{-1}$. Since

$$(P^*)^2 = \begin{pmatrix} 7 & 2 & 2 & 2 & 2 & 4 & 2 & 4 & 2 & 2 & 4 & 4 & 2 & 4 & 4 & 2 \\ 2 & 7 & 2 & 2 & 4 & 2 & 4 & 2 & 2 & 2 & 4 & 4 & 4 & 2 & 2 & 4 \\ 2 & 2 & 7 & 2 & 2 & 4 & 2 & 4 & 4 & 4 & 2 & 2 & 4 & 2 & 2 & 4 \\ 2 & 2 & 2 & 7 & 4 & 2 & 4 & 2 & 4 & 4 & 2 & 2 & 2 & 4 & 4 & 2 \\ 2 & 4 & 2 & 4 & 7 & 2 & 2 & 2 & 2 & 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 2 & 4 & 2 & 2 & 7 & 2 & 2 & 4 & 2 & 2 & 4 & 2 & 2 & 4 & 4 \\ 2 & 4 & 2 & 4 & 2 & 2 & 7 & 2 & 4 & 2 & 2 & 4 & 4 & 4 & 2 & 2 \\ 4 & 2 & 4 & 2 & 2 & 2 & 2 & 7 & 2 & 4 & 4 & 2 & 4 & 4 & 2 & 2 \\ 2 & 2 & 4 & 4 & 2 & 4 & 4 & 2 & 7 & 2 & 2 & 2 & 2 & 4 & 2 & 4 \\ 2 & 2 & 4 & 4 & 4 & 2 & 2 & 4 & 2 & 7 & 2 & 2 & 4 & 2 & 4 & 2 \\ 4 & 4 & 2 & 2 & 4 & 2 & 2 & 4 & 2 & 2 & 7 & 2 & 2 & 4 & 2 & 4 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 & 2 & 2 & 2 & 2 & 7 & 4 & 2 & 4 & 2 \\ 2 & 4 & 4 & 2 & 2 & 2 & 4 & 4 & 2 & 4 & 2 & 4 & 7 & 2 & 2 & 2 \\ 4 & 2 & 2 & 4 & 2 & 2 & 4 & 4 & 4 & 2 & 4 & 2 & 2 & 7 & 2 & 2 \\ 4 & 2 & 2 & 4 & 4 & 4 & 2 & 2 & 2 & 4 & 2 & 4 & 2 & 2 & 7 & 2 \\ 2 & 4 & 4 & 2 & 4 & 4 & 2 & 2 & 4 & 2 & 4 & 2 & 2 & 2 & 2 & 7 \end{pmatrix}$$

we have $R_1(P) = R_{-1}(P) = 2$. Therefore, we have

Proposition 2. *There does not exist any impossible differential or zero correlation linear hull of $\mathcal{E}^{ARIA}$ which covers $r \geq 5$ rounds. Or equivalently, there does not exist any 5-round impossible differential or zero correlation linear hull of the ARIA unless the details of the S-boxes are considered.*

Since we already have 4-round impossible differential and 4-round zero correlation linear hull of $\mathcal{E}^{AES}$ and $\mathcal{E}^{ARIA}$, unless we investigate on the details of the S-boxes, with respect to the rounds, we cannot find neither better impossible differentials nor zero correlation linear hulls for the AES and ARIA.

5 Cryptanalysis of Feistel Structures with SP-Type Round Functions

In the following, we simply use $\mathcal{F}_{SP}^{(r)}$ to denote an r-round Feistel structure with SP-type round functions. Since the techniques to study the Feistel structure with SPN round functions are almost the same, we only give the results as follows.

Lemma 2. *Assume $m \leq 2^{b-1}-1$. If $(\alpha_1, \beta_1) \to (\gamma_1, \alpha_1)$ and $(\alpha_2, \beta_2) \to (\gamma_2, \alpha_2)$ are possible differentials of $\mathcal{F}_{SP}^{(1)}$. Then, there always exist α, β and γ, such that $\chi(\alpha) = \chi(\alpha_1)|\chi(\alpha_2)$, $\chi(\beta) = \chi(\beta_1)|\chi(\beta_2)$, $\chi(\gamma) = \chi(\gamma_1)|\chi(\gamma_2)$, and $(\alpha, \beta) \to (\gamma, \alpha)$ is a possible differential of $\mathcal{F}_{SP}^{(1)}$.*

We have shown that all impossible differentials of an SPN structure are independent impossible differentials. However, this does not hold for the Feistel structure. In the following, we only consider the independent impossible differentials of a Feistel structure which fits well with most of the practical cases.

Lemma 3. *If $\alpha_1 \to \beta_1$ and $\alpha_2 \to \beta_2$ are independent possible differentials of $\mathcal{F}_{SP}^{(r)}$, $(\alpha_1|\alpha_2) \to (\beta_1|\beta_2)$ is also an independent possible differential.*

Theorem 3. *There exists an independent impossible differential of $\mathcal{F}_{SP}^{(r)}$ if and only if there exists an impossible differential $\alpha \not\to \beta$ of $\mathcal{F}_{SP}^{(r)}$ where $H(\alpha) = H(\beta) = 1$.*

Therefore, checking whether there exists an r-round independent impossible differential of a Feistel structure with SP-type round functions can also be reduced to checking whether there exists an r-round independent impossible differential with the Hamming weights of both the input and output difference being 1. Since the dual structure of $\mathcal{F}_{SP}$ is $\sigma \circ \mathcal{F}_{P^T S} \circ \sigma$, the results on impossible differentials cannot be applied to zero correlation linear hulls directly. However, in case P is invertible, we always have

$$\mathcal{F}_{P^T S} = \left((P^T)^{-1}, (P^T)^{-1}\right) \circ \mathcal{F}_{SP^T} \circ \left(P^T, P^T\right) \triangleq P_{\text{in}} \circ \mathcal{F}_{SP^T} \circ P_{\text{out}},$$

which indicates that despite some linear transformations applied to the input and output masks, respectively, both $\mathcal{F}_{SP}$ and $\mathcal{F}_{SP}^{\perp}$ are Feistel structures with SPN round functions. We use the following definition of independent zero correlation linear hulls for $\mathcal{F}_{SP}$.

Definition 5. *Let $\alpha \not\to \beta$ be a zero correlation linear hull of $\mathcal{F}_{SP}$. If for all α^* and β^* satisfying $\chi(P_{\text{in}}\alpha^*) = \chi(P_{\text{in}}\alpha)$ and $\chi(P_{\text{out}}\beta^*) = \chi(P_{\text{out}}\beta)$, $\alpha^* \not\to \beta^*$ are zero correlation linear hulls, we call $\alpha \not\to \beta$ an* independent zero correlation linear hull *of $\mathcal{F}_{SP}$. Otherwise, we call it a* dependent zero correlation linear hull *of $\mathcal{F}_{SP}$.*

Then based on the links between impossible differentials and zero correlation linear hulls, we have:

Corollary 3. *There exists an independent zero correlation linear hull of $\mathcal{F}_{SP}^{(r)}$ if and only if there exists an independent zero correlation linear hull $\alpha \not\to \beta$ of $\mathcal{F}_{SP}^{(r)}$ where $H(P_{\text{in}}\alpha) = H(P_{\text{out}}\beta) = 1$.*

Theorem 4. *Let $R_2(P)$ be the type 2 primitive indexes of P. Then, there does not exist any independent impossible differential or zero correlation linear hull of $\mathcal{F}_{SP}^{(r)}$ for $r \geq 2R_2(P) + 5$.*

The proof is similar with the SPN structures. The key point is that, as in the proof of Lemma 1, we can always choose $\beta_1, \beta_2, \gamma_1, \gamma_2$ and φ, where $H(\beta_1) = H(\beta_2) = H(\varphi) = m$ such that the differential shown in Fig.3 is a possible one.

To avoid some potential attack, an FL/FL^{-1} layer is inserted to the Feistel structure every 6 rounds in Camellia. Denote by $\mathcal{E}^{Camellia*}$ the structure deduced by Camellia without the FL/FL^{-1} layer. Since

$$(P^*)^2 + I = \begin{pmatrix} 4 & 3 & 5 & 4 & 5 & 5 & 4 & 4 \\ 4 & 4 & 3 & 5 & 4 & 5 & 5 & 4 \\ 5 & 4 & 4 & 3 & 4 & 4 & 5 & 5 \\ 3 & 5 & 4 & 4 & 5 & 4 & 4 & 5 \\ 3 & 2 & 3 & 4 & 5 & 3 & 4 & 4 \\ 4 & 3 & 2 & 3 & 4 & 5 & 3 & 4 \\ 3 & 4 & 3 & 2 & 4 & 4 & 5 & 3 \\ 2 & 3 & 4 & 3 & 3 & 4 & 4 & 5 \end{pmatrix},$$

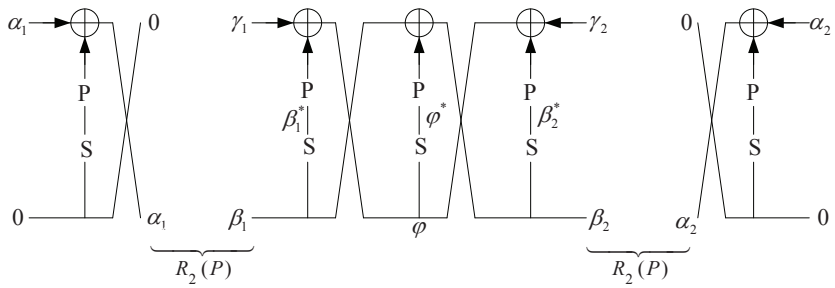

Fig. 3. Constructing $(2R_2(P) + 5)$-round differential for $\mathcal{F}_{SP}$

where I is the identity matrix, we have $R_2(P) = 2$. Therefore, we obtain the following proposition:

Proposition 3. *There does not exist any independent impossible differential of* $\mathcal{E}^{Camellia^*}$ *which covers* $r \geq 9$ *rounds. Or equivalently, there does not exist any* 9*-round independent impossible differential of Camellia without* FL/FL^{-1} *unless the details of the S-boxes are considered.*

In other words, unless we investigate the details of the S-boxes, the known independent impossible differentials of Camellia without FL/FL^{-1} cannot be improved with respect to the rounds.

Zodiac is another Feistel cipher with SP-type round function. Please refer to [11, 15] for more details of Zodiac. Since we have $R_2(P) = 6$, if we do not exploit the details of the S-boxes, there does not exist any $2 \times 6 + 5 = 17$ independent impossible differential of Zodiac, while the longest impossible differential of Zodiac is 16 rounds[22].

Although there may exist some dependent impossible differentials of Feistel structures with SP-type round functions, we believe that the bound given above is also applicable to all impossible differentials.

6 Conclusion

In this paper, we mainly investigated the security of structures against impossible differential and zero correlation linear cryptanalysis. Our approach is to determine an upper bound for the longest impossible differentials for a structure. We first reduced the problem whether there exists an r-round impossible differential to the problem whether there exists an r-round impossible differential where the Hamming weights of the input and output differentials are 1. Therefore, we reduced the time complexity of checking whether there exists an impossible differential of an SPN structure or an independent impossible differential of a Feistel structure with SP-type round functions from $\mathcal{O}(2^{2m})$ to $\mathcal{O}(m^2)$. Then, by using the structures and dual structures, as well as the matrices theory, we have

given an upper bound for the rounds of impossible differentials and zero correlation linear hulls for both SPN structures and Feistel structures with SP-type round functions.

As in the provable security of differential and linear cryptanalysis, we gave an upper bound on the longest rounds of the impossible differentials that are independent of the choice of the non-linear components. Although we are only interested in the truncated impossible differentials, we believe that this kind of impossible differentials cover most of the known cases. Therefore, they not only have theoretical significance, but also have practical significance. As a result, see Table 1, we show that unless the details of the non-linear layer are considered, there does not exist any 5-round impossible differentials of the AES or ARIA, and there does not exist any 9-round independent impossible differentials of the Camellia without FL/FL^{-1} layer.

Table 1. Known results for some block ciphers

	Bound	Known rounds	Reference	
AES	4	4	[19]	
ARIA	4	4	[25]	
Camellia	8	8	[25]	independent ID
Zodiac	16	16	[22]	independent ID

Acknowledgment

The authors would like to thank the anonymous reviewers for their useful comments, and Shaojing Fu, Lei Cheng and Xuan Shen for fruitful discussions.

References

1. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. In Stinson, D.R., Tavares, S.E., eds.: Selected Areas in Cryptography 2000. Volume 2012 of LNCS., Springer (2000) 39–56
2. Aumasson, J., Guo, J., Knellwolf, S., Matusiewicz, K., Meier, W.: Differential and Invertibility Properties of BLAKE. In Hong, S., Iwata, T., eds.: Fast Software Encryption 2010. Volume 6147 of Lecture Notes in Computer Science., Springer (2010) 318–332
3. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In Stern, J., ed.: EUROCRYPT '99. Volume 1592 of LNCS., Springer (1999) 12–23

4. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer (1993)
5. Blondeau, C.: Impossible differential attack on 13-round Camellia-192. Inf. Process. Lett. **115**(9) (2015) 660–666
6. Bogdanov, A., Rijmen, V.: Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Des. Codes Cryptography **70**(3) (2014) 369–383
7. Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon. In Sarkar, P., Iwata, T., eds.: ASIACRYPT 2014. Volume 8873 of LNCS., Springer (2014) 179–199
8. Daemen, J., Rijmen, V.: AES and the Wide Trail Design Strategy. In Knudsen, L.R., ed.: EUROCRYPT 2002. Volume 2332 of LNCS., Springer (2002) 108–109
9. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Springer (2002)
10. Guo, J., Thomsen, S.S.: Deterministic Differential Properties of the Compression Function of BMW. In Biryukov, A., Gong, G., Stinson, D.R., eds.: Selected Areas in Cryptography 2010. Volume 6544 of Lecture Notes in Computer Science., Springer (2010) 338–350
11. Hong, D., Sung, J., Moriai, S., Lee, S., Lim, J.: Impossible Differential Cryptanalysis of Zodiac. In Matsui, M., ed.: Fast Software Encryption 2001. Volume 2355 of LNCS., Springer (2001) 300–311
12. Kim, J., Hong, S., Lim, J.: Impossible differential cryptanalysis using matrix method. Discrete Mathematics **310**(5) (2010) 988–1002
13. Knudsen, L.R.: DEAL – A 128-bit Block Cipher. Technical report, Department of Informatics, University of Bergen, Norway (1998)
14. Kwon, D., Kim, J., Park, S., Sung, S.H., Sohn, Y., Song, J.H., Yeom, Y., Yoon, E., Lee, S., Lee, J., Chee, S., Han, D., Hong, J.: New Block Cipher: ARIA. In Lim, J.I., Lee, D.H., eds.: ICISC 2003. Volume 2971 of LNCS., Springer (2003) 432–445
15. Lee, C., Jun, K., MinSukJung, Park, S., Kim, J.: Zodiac Version 1.0(revised) Architecture and Specification. In: Standardization Workshop on Information Security Technology 2000, Korean Contribution on MP18033, ISO/IEC JTC1/SC27 N2563, 2000, http://www.kisa.or.kr/seed/index.html. (2000)
16. Li, R., Sun, B., Li, C.: Impossible differential cryptanalysis of SPN ciphers. IET Information Security **5**(2) (2011) 111–120
17. Lu, J., Dunkelman, O., Keller, N., Kim, J.: New Impossible Differential Attacks on AES. In Chowdhury, D.R., Rijmen, V., Das, A., eds.: INDOCRYPT 2008. Volume 5365 of LNCS., Springer (2008) 279–293
18. Luo, Y., Lai, X., Wu, Z., Gong, G.: A unified method for finding impossible differentials of block cipher structures. Inf. Sci. **263** (2014) 211–220
19. Mala, H., Dakhilalian, M., Rijmen, V., Modarres-Hashemi, M.: Improved Impossible Differential Cryptanalysis of 7-Round AES-128. In Gong, G., Gupta, K.C., eds.: INDOCRYPT 2010. Volume 6498 of LNCS., Springer (2010) 282–291
20. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In Helleseth, T., ed.: EUROCRYPT '93. Volume 765 of LNCS., Springer (1993) 386–397
21. Sun, B., Liu, Z., Rijmen, V., Li, R., Cheng, L., Wang, Q., AlKhzaimi, H., Li, C.: Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis. In Gennaro, R., Robshaw, M., eds.: CRYPTO 2015. Volume 9215 of LNCS., Springer (2015) 95–115
22. Sun, B., Zhang, P., Li, C.: Impossible Differential and Integral Cryptanalysis of Zodiac. Journal of Software **22**(8) (2011) 1911–1917

23. Vaudenay, S.: Provable Security for Block Ciphers by Decorrelation. In Morvan, M., Meinel, C., Krob, D., eds.: STACS 98. Volume 1373 of LNCS., Springer (1998) 249–275
24. Wu, S., Wang, M.: Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers. In Galbraith, S.D., Nandi, M., eds.: INDOCRYPT 2012. Volume 7668 of LNCS., Springer (2012) 283–302
25. Wu, W., Zhang, W., Feng, D.: Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia. J. Comput. Sci. Technol. **22**(3) (2007) 449–456

A Proof of Lemma 1.

Firstly, $\alpha_1 \to \beta_1$ and $\alpha_2 \to \beta_2$ are possible differentials of $\mathcal{E}^{SP}$ implies that there exist some α_1^*, α_2^*, $\chi(\alpha_1^*) = \chi(\alpha_1)$, $\chi(\alpha_2^*) = \chi(\alpha_2)$, such that the following differentials hold:

$$\begin{cases} \alpha_1 \xrightarrow{S} \alpha_1^* \xrightarrow{P} \beta_1, \\ \alpha_2 \xrightarrow{S} \alpha_2^* \xrightarrow{P} \beta_2. \end{cases}$$

For any $\lambda \in \mathbb{F}_{2^b}^*$, since $\chi(\lambda\alpha_2^*) = \chi(\alpha_2)$, $\alpha_2 \xrightarrow{S} \lambda\alpha_2^* \xrightarrow{P} \lambda\beta_2$ is also a possible differential of $\mathcal{E}^{SP}$.

Without loss of generality, let

$$\begin{cases} \alpha_1^* = (x_{w_1}^{(1)}, x_{r_1}^{(1)}, 0_{m-r_1-w_1}) \\ \alpha_2^* = (x_{w_1}^{(2)}, 0_{r_1}, x_{m-r_1-w_1}^{(2)}) \\ \beta_1 = (y_{w_2}^{(1)}, y_{r_2}^{(1)}, 0_{m-r_2-w_2}) \\ \beta_2 = (y_{w_2}^{(2)}, 0_{r_2}, y_{m-r_2-w_2}^{(2)}) \end{cases}$$

where $0_t = \underbrace{0 \cdots 0}_{t}$, $x_r^{(i)}, y_r^{(i)} \in (\mathbb{F}_{2^b}^*)^r$. Let

$$\begin{cases} x_{w_1}^{(1)} = (a_0^{(1)}, \ldots, a_{w_1-1}^{(1)}) \\ x_{w_1}^{(2)} = (a_0^{(2)}, \ldots, a_{w_1-1}^{(2)}) \\ y_{w_2}^{(1)} = (b_0^{(1)}, \ldots, b_{w_2-1}^{(1)}) \\ y_{w_2}^{(2)} = (b_0^{(2)}, \ldots, b_{w_2-1}^{(2)}) \end{cases}$$

and let

$$\Lambda = \left\{ \frac{a_0^{(1)}}{a_0^{(2)}}, \ldots, \frac{a_{w_1-1}^{(1)}}{a_{w_1-1}^{(2)}}, \frac{b_0^{(1)}}{b_0^{(2)}}, \ldots, \frac{b_{w_2-1}^{(1)}}{b_{w_2-1}^{(2)}} \right\}.$$

Since $\#\Lambda \le w_1 + w_2 \le m + m = 2m \le 2 \times (2^{b-1} - 1) = 2^b - 2$, $\mathbb{F}_{2^b}^* \setminus \Lambda$ is a non-empty set. Therefore, for $\lambda \in \mathbb{F}_{2^b}^* \setminus \Lambda$, we always have

$$\begin{cases} \chi(\alpha_1^* \oplus \lambda\alpha_2^*) = \chi(\alpha_1^* | \alpha_2^*) \\ \chi(\beta_1 \oplus \lambda\beta_2) = \chi(\beta_1 | \beta_2), \end{cases}$$

which implies that

$$\alpha_1|\alpha_2 \xrightarrow{\mathcal{S}} \alpha_1^* \oplus \lambda\alpha_2^* \xrightarrow{P} \beta_1 \oplus \lambda\beta_2$$

is a possible differential of $\mathcal{E}^{SP}$.