Security Analysis of the GF-NLFSR Structure and Four-Cell Block Cipher

Wenling Wu, Lei Zhang, Liting Zhang, and Wentao Zhang

State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences, Beijing 100190, P.R. China
wwl@is.iscas.ac.cn

Abstract. The overall structure is one of the most important properties of block ciphers. At present, the most common structures include Feistel structure, SP structure, MISTY structure, L-M structure and Generalized Feistel structure. In [29], Choy et al. proposed a new structure called GF-NLFSR (Generalized Feistel-NonLinear Feedback Shift Register), and designed a new block cipher called Four-Cell which is based on the 4-cell GF-NLFSR. In this paper, we first study properties of the n-cell GF-NLFSR structure, and prove that for an n-cell GF-NLFSR, there exists an (n^2+n-2) rounds impossible differential. Then we present an impossible differential attack on the full 25-round Four-Cell using this kind of 18-round impossible differential distinguisher together with differential cryptanalysis technique. The data complexity of our attack is $2^{111.5}$ and the time complexity is less than $2^{123.5}$ encryptions. In addition, we expect the attack to be more efficient when the relations between different round subkeys can be exploited by taking the key schedule algorithm into consideration.

Keywords: GF-NLFSR structure, Four-Cell block cipher, Impossible differential cryptanalysis, Data complexity, Time complexity.

1 Introduction

The overall structure is one of the most important properties of block ciphers, and it plays important roles in the round number choice, software and hardware implementation performances and so on. At present, the most often used structures include Feistel structure, SP structure, MISTY structure, L-M structure and Generalized Feistel structure. Feistel structure was introduced by H. Feistel in the design of Lucifer block cipher and later got famous since it was used in the design of DES. Feistel structure can transfer any function (usually called round function F) to a permutation. Now there are a lot of block ciphers employing the Feistel structure, such as Camellia, FEAL, GOST, LOKI, E2, Blowfish, RC5 and so on. The security of Feistel structure against differential and linear cryptanalysis was evaluated by many researchers, for example [1,2,3], and meanwhile there are many results such as [4,5,6,7,8,9,10] about the pseudorandomness of Feistel structure. Besides the Feistel structure, the other most often used structure is the SP structure, the well known block ciphers such as AES, Serpent

S. Qing, C.J. Mitchell, and G. Wang (Eds.): ICICS 2009, LNCS 5927, pp. 17–31, 2009.
© Springer-Verlag Berlin Heidelberg 2009

and ARIA all employ the SP structure. In each round of the SP structure, first a layer of key-dependent inversive function named S is applied to the input, and then applies a permutation or an inversive linear transformation named P. Hence the SP structure is very simple and clear, and S is usually called the confusion layer which achieves confusion in the cipher and P is usually referred to as the diffusion layer which diffuses efficiently. MISTY structure is another kind of important structures which was proposed by M. Matsui in [11], and it was used in the design of the block ciphers MISTY [12] and KASUMI [13]. There are many results about the security analysis of the MISTY structure such as in [14,15,16,17]. S. Vaudenay et al. named the structure of the block cipher IDEA as the L-M structure or Lai-Massey structure [18], and the FOX [19] cipher also employs a variant of the L-M structure. The generalized Feistel structure was first introduced by B. Schneier and J. Kelsey which can be considered as an unbalanced Feistel structure[20], and then many variants of generalized Feistel structure are proposed such as CAST-256-type [21], MARS-type [22], SMS4-type [23], CLEFIA-type [24] and so on. All these kinds of generalized Feistel structures have similar advantages such as decryption - encryption similarity and the inverse of round function is not necessary in decryption. Furthermore, this can make the design of round function more simple and flexible. The security analysis of generalized Feistel structure is very important when they are used to design new block ciphers, and there are many results [25,26,27,28] about the security of different kinds of generalized Feistel structures against the differential and linear cryptanalysis and also their pseudorandomness.

In [29], Choy et al. proposed a new structure called GF-NLFSR (Generalized Feistel-NonLinear Feedback Shift Register). It can be considered as an n-cell extension of combining the MISTY structure and Generalized Unbalanced Feistel Network together. The security of the structure against many attacks such as differential, linear, impossible differential and integral cryptanalysis are also considered in [29]. For an n-cell GF-NLFSR, an upper bound for the differential and linear hull probabilities for any $n+1$ rounds are given, and a $2n-1$ rounds impossible differential distinguisher and a $3n-1$ rounds integral distinguisher on the n-cell GF-NLFSR are demonstrated. Furthermore, a new block cipher called Four-Cell which is based on the 4-cell GF-NLFSR was designed in [29]. The block and key size of Four-Cell are both 128-bit, and there are 25 rounds in total.

Impossible differential cryptanalysis [30] was first proposed by Biham, Biryukov and Shamir in 1999, and it was applied to analyze the Skipjack block cipher. Unlike differential cryptanalysis which exploits differentials with the highest possible probability, impossible differential cryptanalysis uses the differentials which hold with probability 0, which can thus be called impossible differential. The impossible differentials can usually be built in a miss-in-the-middle manner. Recently, impossible differential cryptanalysis had received worldwide attention, and its application to block ciphers such as AES, Camellia and MISTY all achieved very good results [31,32,33,34,35].

In [29], Proposition 3 stated that for an n-cell GF-NLFSR, there exist at most $2n-1$ rounds impossible differential distinguishers using the U-method proposed

in [36]. However, we examine the property of n-cell GF-NLFSR structure and demonstrate that there exists a (n^2+n-2) rounds impossible differential distinguisher. Then we present an impossible differential attack on the full 25-round Four-Cell using this kind of 18-round impossible differential distinguisher together with differential cryptanalysis technique.

This paper is organized as follows. In Section 2, we give a brief description of the n-cell GF-NLFSR structure and Four-Cell block cipher. In Section 3, we describe some useful properties of the n-cell GF-NLFSR structure and the (n^2+n-2) rounds impossible differential. Then in Section 4, we present our impossible differential attack on the full 25-round Four-Cell block cipher. Finally, in Section 5 we summarize this paper.

2 The n-Cell GF-NLFSR Structure and Four-Cell Block Cipher

2.1 The n-Cell GF-NLFSR Structure

In this section, we will give a brief description of the n-cell GF-NLFSR structure, and Fig. 1 below illustrates one round of GF-NLFSR.

For an n-cell GF-NLFSR structure, suppose the size of the internal sub-block is m-bit, and then we can denote the mn-bit input block as $(x_1, x_2, x_3, ..., x_n) \in (\{0,1\}^m)^n$. If we denote the round subkey as sk, then the output of one round n-cell GF-NLFSR transformation is defined as follows.

$$\begin{aligned} &x_2 = x_2,\\ &x_3 = x_3,\\ &\cdots\\ &x_n = x_n,\\ &x_{n+1} = f(x_1, sk) \oplus x_2 \oplus x_3 ... \oplus x_n, \end{aligned}$$

where the output block is denoted as $(x_2, x_3, ..., x_n, x_{n+1}) \in (\{0,1\}^m)^n$. Note here the symbol $\oplus$ is used to denote finite field addition (XOR) over $GF(2)^m$, and the function $f : \{0,1\}^m \times \{0,1\}^k \to \{0,1\}^m$ is the round function. Specifically, for each fixed round key sk, the round function $f(\cdot, sk) : \{0,1\}^m \to \{0,1\}^m$ must be a permutation, or else the n-cell GF-NLFSR structure is not able to decrypt correctly. Therefore, in our later analysis, we will assume the round function f is a permutation when the round key is fixed.

2.2 Four-Cell Block Cipher

The block and key size of Four-Cell are both 128-bit, and it uses the 4-cell GF-NLFSR structure. Since the designers only give a rough suggestion for the key schedule algorithm, namely using a similar cipher with 26 rounds to generate the round keys needed. Hence in this paper, we will omit the key schedule and just assume that the round keys are randomly chosen. The encryption algorithm of Four-Cell can be described briefly as follows.

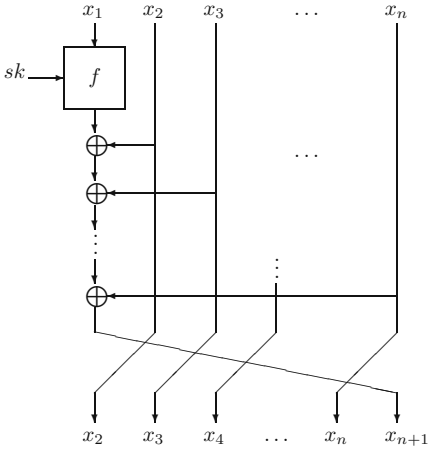

Fig. 1. One Round of n-Cell GF-NLFSR structure

Let the plaintext be denoted by $P = (x_1, x_2, x_3, x_4) \in (\{0,1\}^{32})^4$, then after applying the full 25 rounds encryption, the 128-bit ciphertext can be denoted by C. Let $(x_i, x_{i+1}, x_{i+2}, x_{i+3}) \in (\{0,1\}^{32})^4$ denote the input of the i-th round, then the output of the i-th round can be computed as follows.

$$\begin{aligned} x_{i+1} &= x_{i+1}, \\ x_{i+2} &= x_{i+2}, \\ x_{i+3} &= x_{i+3}, \\ x_{i+4} &= f_i(x_i, sk_i) \oplus x_{i+1} \oplus x_{i+2} \oplus x_{i+3}. \end{aligned}$$

For rounds $i = 1, 2, .., 5$ and $i = 21, 22, .., 25$, the round keys are denoted as $sk_i \in \{0,1\}^{32}$ and the round function is defined as $f_i(x_i, sk_i) = MDS(S(x_i \oplus sk_i))$. For rounds $i = 6, 7, .., 20$, the round keys are denoted as $sk_i = (sk_{i0}, sk_{i1}) \in (\{0,1\}^{32})^2$, and the round function is defined as $f_i(x_i, sk_i) = S(MDS(S(x_i \oplus sk_{i0})) \oplus sk_{i1})$.

Here in each round function, $S : (\{0,1\}^8)^4 \to (\{0,1\}^8)^4$ is four parallel 8×8 s-boxes, and the s-box is similar with the s-box used in the SubBytes operation in AES. The transformation $MDS : (\{0,1\}^8)^4 \to (\{0,1\}^8)^4$ is a 4-byte to 4-byte maximal distance separable transform with optimal branch number 5, and it is similar with the MixColumn operation in AES. In the end, the output after 25 rounds is XORed with a 128-bit post-whitening key $K_{26} = (k_{26}^1, k_{26}^2, k_{26}^3, k_{26}^4)$ to get the ciphertext, namely $C = (x_{26} \oplus k_{26}^1, x_{27} \oplus k_{26}^2, x_{28} \oplus k_{26}^3, x_{29} \oplus k_{26}^4)$.

3 Differential Property of the n-Cell GF-NLFSR Structure

For the n-cell GF-NLFSR structure, we can express the nm-bit input as n words which consists of m bits each. Suppose we have a pair of plaintexts

$X = (x_1, x_2, x_3, ..., x_n)$ and $X^* = (x_1^*, x_2^*, x_3^*, ..., x_n^*)$, and their difference is denoted by $\Delta X = (\Delta x_1, \Delta x_2, ..., \Delta x_n)$, where $\Delta x_1 = x_1 \oplus x_1^*, ..., \Delta x_n = x_n \oplus x_n^*$. Note the symbol 0 in the difference $\Delta X = (\Delta x_1, \Delta x_2, \Delta x_3, 0, ..., 0)$ means that the corresponding byte difference is zero.

Lemma 1. *For the n-cell GF-NLFSR structure, there exists the following n rounds differential characteristic whose probability is equal to 1.*

$$(\Delta x_1, \Delta x_2, ..., \Delta x_{i-1}, \Delta x_i, 0, ..., 0) \xrightarrow{n \text{ rounds}} (\Delta y_1, \Delta y_2, ..., \Delta y_i, \Delta y_{i+1}, 0, ..., 0).$$

We denote this kind of differential characteristic as Δ_i, where $1 \leq i \leq n-1$, and these differential characteristics Δ_i satisfy the following two properties.

1. $\Delta y_1 \oplus \Delta y_2 \oplus ... \oplus \Delta y_i \oplus \Delta y_{i+1} = 0$.
2. *If* $\Delta x_i \neq 0$, *then* $\Delta y_{i+1} \neq 0$.

Proof. Let the round function of Round i be $f_{sk_i}(x_i) = f_i(x_i, sk_i)$. Then when the round key sk_i is fixed, the round function f_{sk_i} must be a permutation, or else one can not decrypt correctly for the n-cell GF-NLFSR structure. According to the structure of the n-cell GF-NLFSR, we can get the following equations which are illustrated in Table 1.

$$\Delta y_1 = f_{sk_1}(x_1) \oplus f_{sk_1}(x_1 \oplus \Delta x_1) \oplus \Delta x_2 \oplus ... \oplus \Delta x_i \tag{1}$$

$$\Delta y_i = f_{sk_i}(x_i) \oplus f_{sk_i}(x_i \oplus \Delta x_i) \oplus \Delta y_1 \oplus ... \oplus \Delta y_{i-1} \tag{2}$$

$$\Delta y_{i+1} = \Delta y_1 \oplus ... \oplus \Delta y_{i-1} \oplus \Delta y_i \tag{3}$$

Table 1. The n rounds differential characteristic of the n-cell GF-NLFSR structure

Round\Diff.	Δx_1	Δx_2	...	Δx_{i-1}	Δx_i	0	...	0
1	Δx_2	Δx_3	...	Δx_i	0	...	0	Δy_1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$i-1$	Δx_i	0	...	0	0	Δy_1	...	Δy_{i-1}
i	0	...	0	0	Δy_1	...	Δy_{i-1}	Δy_i
$i+1$	0	...	0	Δy_1	...	Δy_{i-1}	Δy_i	Δy_{i+1}
$i+2$	0	...	Δy_1	...	Δy_{i-1}	Δy_i	Δy_{i+1}	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
n	Δy_1	Δy_2	...	Δy_i	Δy_{i+1}	0	...	0

According to Equ. (3), the following one round differential characteristic will hold with probability 1.

$$(0, ..., 0, \Delta y_1, ..., \Delta y_{i-1}, \Delta y_i, \Delta y_{i+1}) \xrightarrow{1 \text{ round}} (0, ..., 0, \Delta y_1, ..., \Delta y_i, \Delta y_{i+1}, 0).$$

Similarly, we can know that all the differential characteristics from Round $(i+2)$ to Round n in Table 1 hold with probability 1. Therefore, for the n-cell GF-NLFSR structure, there exists the following n rounds differential characteristic and its probability is equal to 1.

$$(\Delta x_1, \Delta x_2, ..., \Delta x_{i-1}, \Delta x_i, 0, ..., 0) \xrightarrow{n \text{ rounds}} (\Delta y_1, \Delta y_2, ..., \Delta y_i, \Delta y_{i+1}, 0, ..., 0)$$

Then according to Equ. (3), we can easily get the first property, i.e. $\Delta y_1 \oplus \Delta y_2 \oplus ... \oplus \Delta y_i \oplus \Delta y_{i+1} = 0$. Therefore, in the following we only need to prove the second property.

According to Equ. (2) and Equ. (3), we can get the following equation.

$$\Delta y_{i+1} = \Delta y_1 \oplus ... \oplus \Delta y_{i-1} \oplus \Delta y_i = f_{sk_i}(x_i) \oplus f_{sk_i}(x_i \oplus \Delta x_i).$$

When $\Delta x_i \neq 0$, we can conclude that $f_{sk_i}(x_i) \oplus f_{sk_i}(x_i \oplus \Delta x_i) \neq 0$ since the function f_{sk_i} is a permutation. Therefore, we get the second property, namely if $\Delta x_i \neq 0$, then $\Delta y_{i+1} \neq 0$. □

Lemma 2. *For the inverse of the n-cell GF-NLFSR structure which is denoted as the n-cell GF-NLFSR^{-1} structure, there exists the following $(2n-2)$ rounds differential characteristic whose probability is equal to 1.*

$$(\beta, \beta, 0, ..., 0) \xrightarrow{2n-2 \text{ rounds}} (?, ..., ?, b_2, b_1, 0).$$

We denote this kind of differential characteristic as Δ_{β}^{-1}, where the symbol ? denotes an unknown difference and β, b_2, b_1 denote non-zero differences.

Proof. According to the structure of the n-cell GF-NLFSR^{-1}, we can get the following one round differential characteristic which holds with probability 1, and this kind of differential is illustrated in Table 2.

$$(\beta, \beta, 0, ..., 0) \xrightarrow{1 \text{ round}} (0, \beta, \beta, 0, ..., 0).$$

Similarly, all the differential characteristics from the Round 2 to Round $(n-1)$ in Table 2 all hold with probability 1. Then in the Round n, if we denote the

Table 2. The $(2n-2)$ rounds differential of the n-cell GF-NLFSR^{-1} structure

Round\Diff.	β	β	0	0	...	0
1	0	β	β	0	...	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
$n-2$	0	0	...	0	β	β
$n-1$	0	0	...	0	0	β
n	b_1	0	0	...	0	0
$n+1$	b_2	b_1	0	...	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
$2n-2$	?	...	?	b_2	b_1	0

round function as g_n, then $b_1 = g_n(z) \oplus g_n(z \oplus \beta)$. Because the difference β is non-zero and the function g_n is a permutation, we can conclude that $b_1 \neq 0$. Similarly, in the $(n+1)$-th round we have $b_2 = g_{n+1}(w) \oplus g_{n+1}(w \oplus b_1)$, and thus we can conclude that $b_2 \neq 0$ since $b_1 \neq 0$.

Finally, according to the property of the n-cell GF-NLFSR^{-1} structure, the differential characteristics from Round $(n+2)$ to Round $(2n-2)$ in Table 2 all hold with probability 1. Therefore, for the n-cell GF-NLFSR^{-1} structure, there exists the following differential characteristic whose probability is equal to 1.

$$(\beta, \beta, 0, ..., 0) \xrightarrow{2n-2 \text{ rounds}} (?, ..., ?, b_2, b_1, 0). \qquad \square$$

Theorem 1. *For the n-cell GF-NLFSR structure, there exists the following kind of (n^2+n-2) rounds impossible differential where α and β are non-zero differences.*

$$(\alpha, 0, ..., 0) \xrightarrow{n^2+n-2 \text{ rounds}} (\beta, \beta, 0, ..., 0).$$

Proof. This kind of (n^2+n-2) rounds impossible differential is constructed using the miss-in-the-middle technique. First we construct an $n(n-1)$ rounds differential characteristic of the encryption direction and an $(2n-2)$ rounds differential characteristic of the decryption direction whose probabilities are both equal to 1. Then if these two differential characteristics contradict each other in the middle, we get the (n^2+n-2) rounds impossible differential. In Table 3 we illustrate this kind of impossible differential in detail.

When we choose the input difference as $(\alpha, 0, ..., 0)$, we can construct an $n(n-1)$ rounds differential with probability 1 as follows. First of all, based on Lemma 1, we can construct the following n rounds differential Δ_1 whose probability is equal to 1.

$$(\alpha, 0, ..., 0) \xrightarrow{n \text{ rounds}} (\Delta x_1^2, \Delta x_2^2, 0, ..., 0).$$

Since the input difference α is non-zero, according to property 1 and 2 of Lemma 1, we know that Δx_2^2 is also non-zero and $\Delta x_1^2 \oplus \Delta x_2^2 = 0$.

Then, we start with the input difference of $(\Delta x_1^2, \Delta x_2^2, 0, ..., 0)$, and according to Lemma 1, we can construct again an n rounds differential Δ_2 whose probability is 1 as follows.

$$(\Delta x_1^2, \Delta x_2^2, 0, ..., 0) \xrightarrow{n \text{ rounds}} (\Delta x_1^3, \Delta x_2^3, \Delta x_3^3, 0, ..., 0).$$

Since Δx_2^2 is non-zero, we know that $\Delta x_3^3 \neq 0$ and $\Delta x_1^3 \oplus \Delta x_2^3 \oplus \Delta x_3^3 = 0$. Similarly, we can construct the i-th $(3 \leq i \leq n-1)$ n rounds differential Δ_i in turn. In the end, the $(n-1)$-th n rounds differential Δ_{n-1} is as follows, and we can conclude that $\Delta x_n^n \neq 0$ and $\Delta x_1^n \oplus \Delta x_2^n \oplus \Delta x_3^n \oplus ... \oplus \Delta x_n^n = 0$.

$$(\Delta x_1^{n-1}, \Delta x_2^{n-1}, ..., \Delta x_{n-1}^{n-1}, 0) \xrightarrow{n \text{ rounds}} (\Delta x_1^n, \Delta x_2^n, \Delta x_3^n, ..., \Delta x_n^n).$$

By concatenating the above differentials together, we can get the following $n(n-1)$ rounds differential whose probability is equal to 1 and Δx_n^n is non-zero.

$$(\alpha, 0, ..., 0) \xrightarrow{n(n-1) \text{ rounds}} (\Delta x_1^n, \Delta x_2^n, \Delta x_3^n, ..., \Delta x_n^n).$$

Table 3. The (n^2+n-2) rounds impossible differential of n-cell GF-NLFSR structure

Round\Diff.	α	0	0	...	0	0
1	0	0	0	...	0	Δx_1^2
2	0	0	...	0	Δx_1^2	Δx_2^2
3	0	...	0	Δx_1^2	Δx_2^2	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
n	Δx_1^2	Δx_2^2	0	...	0	0
$n+1$	Δx_2^2	0	0	...	0	Δx_1^3
$n+2$	0	0	...	0	Δx_1^3	Δx_2^3
$n+3$	0	...	0	Δx_1^3	Δx_2^3	Δx_3^3
⋮	⋮	⋮	⋮	⋮	⋮	⋮
$2n$	Δx_1^3	Δx_2^3	Δx_3^3	0	...	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
$n(n-2)$	Δx_1^{n-1}	Δx_2^{n-1}	Δx_3^{n-1}	...	Δx_{n-1}^{n-1}	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
$n(n-1)$	Δx_1^n	Δx_2^n	Δx_3^n	...	Δx_{n-1}^n	Δx_n^n
	?	...	?	b_2	b_1	0
$n(n-1)+1$	?	...	b_2	b_1	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
n^2-3	b_2	b_1	0	0	...	0
n^2-2	b_1	0	0	...	0	0
n^2-1	0	0	...	0	0	β
n^2	0	0	...	0	β	β
⋮	⋮	⋮	⋮	⋮	⋮	⋮
n^2+n-3	0	β	β	0	...	0
n^2+n-2	β	β	0	0	...	0

In the decryption direction, considering the inverse structure n-cell GF-NLFSR^{-1}, we get the following $2n-2$ rounds differential characteristic with probability 1 according to Lemma 2.

$$(\beta, \beta, 0, ..., 0) \xrightarrow{2n-2 \text{ rounds}} (?, ..., ?, b_2, b_1, 0).$$

If we concatenate the above $n(n-1)$ rounds differential of the encryption direction and the $(2n-2)$ rounds differential of the decryption direction together, we can construct the following (n^2+n-2) rounds impossible differential since they contradict each other at Δx_n^n.

$$(\alpha, 0, 0, ..., 0) \overset{(n^2+n-2) \text{ rounds}}{\nrightarrow} (\beta, \beta, 0, ..., 0). \qquad \square$$

4 Security Analysis of Four-Cell Block Cipher

According to Theorem 1, for Four-Cell block cipher which employs the 4-cell GF-NLFSR structure, there exists an 18 rounds impossible differential as follows.

$$(\alpha, 0, 0, 0) \overset{18 \text{ rounds}}{\not\to} (\beta, \beta, 0, 0)$$

By setting the 18-round impossible differential distinguisher in the middle rounds, we can present an impossible differential attack on the full 25-round Four-Cell by analyzing the first 4 rounds before and the last 3 rounds after the distinguisher. Note the round functions of the first 5 rounds and the last 5 rounds are all defined as $f_i(x_i, sk_i) = MDS(S(x_i \oplus sk_i))$.

Let the plaintext be $X = (x_1, x_2, x_3, x_4) \in (\{0,1\}^{32})^4$, then the intermediate state after 3 rounds and 4 rounds encryption can be denoted as (x_4, x_5, x_6, x_7) and (x_5, x_6, x_7, x_8) respectively. Furthermore, the intermediate state after 22 rounds encryption can be denoted as $(x_{23}, x_{24}, x_{25}, x_{26})$ and the 128-bit ciphertext should be $C = (c_1, c_2, c_3, c_4) = (x_{26} \oplus k_{26}^1, x_{27} \oplus k_{26}^2, x_{28} \oplus k_{26}^3, x_{29} \oplus k_{26}^4)$. Suppose we choose another plaintext $X^* = (x_1^*, x_2^*, x_3^*, x_4^*) \in (\{0,1\}^{32})^4$, and the plaintext difference can be denoted as $\Delta x_i = x_i \oplus x_i^*$.

Then for the last three rounds of Four-Cell, we have the following equations.

$$\begin{aligned} x_{27} &= MDS(S(x_{23} \oplus sk_{23})) \oplus x_{24} \oplus x_{25} \oplus x_{26}, \\ x_{28} &= MDS(S(x_{24} \oplus sk_{24})) \oplus x_{25} \oplus x_{26} \oplus x_{27}, \\ x_{29} &= MDS(S(x_{25} \oplus sk_{25})) \oplus x_{26} \oplus x_{27} \oplus x_{28}. \end{aligned}$$

If we denote $rk_{25} = k_{26}^1 \oplus k_{26}^2 \oplus k_{26}^3 \oplus k_{26}^4$, then the input of the Sbox layer for Round 25 can be computed as follows.

$$y_{25} = S^{-1}(MDS^{-1}(c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus rk_{25})) = x_{25} \oplus sk_{25}.$$

Similarly, we can denote $rk_{24} = sk_{25} \oplus k_{26}^1 \oplus k_{26}^2 \oplus k_{26}^3$, and compute the input of the Sbox layer for Round 24 as follows.

$$y_{24} = S^{-1}(MDS^{-1}(c_1 \oplus c_2 \oplus c_3 \oplus y_{25} \oplus rk_{24})) = x_{24} \oplus sk_{24}.$$

Finally, for Round 23 the output of the round function is $c_1 \oplus c_2 \oplus y_{24} \oplus y_{25} \oplus sk_{25} \oplus sk_{24} \oplus k_{26}^1 \oplus k_{26}^2$. If we denote $rk_{23} = sk_{24} \oplus sk_{25} \oplus k_{26}^1 \oplus k_{26}^2$, then the input of the round function can be computed in a similar way.

$$y_{23} = S^{-1}(MDS^{-1}(c_1 \oplus c_2 \oplus y_{24} \oplus y_{25} \oplus rk_{23})) = x_{23} \oplus sk_{23}.$$

Therefore, considering that $\Delta x_{23} = \Delta y_{23}$, $\Delta x_{24} = \Delta y_{24}$, $\Delta x_{25} = \Delta y_{25}$ and $\Delta x_{26} = \Delta c_1$, we can obtain the values of $(\Delta x_{23}, \Delta x_{24}, \Delta x_{25}, \Delta x_{26})$ by just computing the values of y_{25}, y_{24} and y_{23} for a pair of ciphertexts $C = (c_1, c_2, c_3, c_4)$ and $C^* = (c_1^*, c_2^*, c_3^*, c_4^*)$.

For the first four rounds of Four-Cell, if we choose the plaintext difference as $(\Delta x_1, \Delta x_2, \Delta x_3, \Delta x_4) = (0, 0, 0, \alpha)$, then we can get the following equations.

$$\begin{aligned} &\Delta x_5 = \alpha, \\ &\Delta x_6 = 0, \\ &\Delta x_7 = 0, \\ &\Delta x_8 = MSD(S(x_4 \oplus sk_4)) \oplus MSD(S(x_4 \oplus \alpha \oplus sk_4)) \oplus \alpha. \end{aligned}$$

Here, $\Delta x_8 = 0$ holds if and only if $S(x_4 \oplus sk_4) \oplus S(x_4 \oplus \alpha \oplus sk_4) = MDS^{-1}(\alpha)$. Because the branch number of MDS is 5, there is at most one passive byte of α. For simplicity, we can assume the last byte of α is passive.

Let $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in (\{0,1\}^8)^4$ and $\beta = (\beta_1, \beta_2, \beta_3, \beta_4) \in (\{0,1\}^8)^4$, and then we will use the symbol $\alpha \xleftrightarrow{S} \beta$ to express that there exists $x_i = (x_{i,1}, x_{i,2}, x_{i,3}, x_{i,4}) \in (\{0,1\}^8)^4$ such that $S(x_i) \oplus S(x_i \oplus \alpha) = \beta$.

Therefore, we can choose a set A which is defined as follows.

$$\mathrm{A} = \{\alpha = (\alpha_1, \alpha_2, \alpha_3, 0) \in (\{0,1\}^8)^4 | \alpha \xleftrightarrow{S} MDS^{-1}(\alpha)\}.$$

Note here the necessary condition for $\alpha \xleftrightarrow{S} MDS^{-1}(\alpha)$ is that α_1, α_2, and α_3 should satisfy a linear relation (e.g. for the MDS used in AES, the linear relation is $0b \cdot \alpha_1 \oplus 0d \cdot \alpha_2 \oplus 09 \cdot \alpha_3 = 0$). Furthermore, for the Sbox of Four-Cell, the probability of $\alpha_i \xleftrightarrow{S} \beta_i$ holds is about 2^{-1} for $\forall \beta_i \in \{0,1\}^8$. Therefore, the set A contains about $|\mathrm{A}| \approx (2^8 - 1) \times (2^8 - 1) \times 2^{-1} \times 2^{-1} \times 2^{-1} \approx 2^{13}$ possible values. We also test this estimation using computer program, and with the same MDS and the Sbox used in AES, our searching result shows that the set A contains $7965 \approx 2^{12.96}$ possible values of α which is very close to the theory estimation.

After analyzing the first four rounds and the last three rounds of Four-Cell, we can set the 18-round impossible differential at Round 5 to Round 22 and apply an impossible differential attack on the full 25-round Four-Cell. The attack procedure consists of three steps, and we will utilize impossible differential attack technique together with some properties of the structure.

The first step of the attack is data collection. We first choose appropriate plaintext structures defined as follows.

$$S_P = \{(a_1, a_2, a_3, x_4)\},$$

where a_1, a_2, a_3 are 32-bit constants and the last byte of x_4 is also an 8-bit constants, namely $x_4 = (x_{4,1}, x_{4,2}, x_{4,3}, a_{4,4}) \in (\{0,1\}^8)^4$, $x_{4,j} \in \{0,1\}^8$. Therefore, each structure contains 2^{24} plaintexts and they can construct about $2^{24} \times 2^{13}/2 \approx 2^{36}$ useful pairs whose plaintext differences satisfy the conditions listed above.

The second step of the attack is data filtering, in which we will discard all the useless pairs which do not satisfy the corresponding ciphertext difference. Note the output difference after the impossible differential distinguisher is $(\Delta x_{23}, \Delta x_{24}, \Delta x_{25}, \Delta x_{26}) = (\beta, \beta, 0, 0)$, and according to the structure of Four-Cell, the ciphertext difference $(\Delta c_1, \Delta c_2, \Delta c_3, \Delta c_4) = (\Delta x_{26}, \Delta x_{27}, \Delta x_{28}, \Delta x_{29})$ should satisfy the following two conditions.

$$\begin{aligned} &\Delta c_1 = 0, \\ &\Delta c_1 \oplus \Delta c_2 \oplus \Delta c_3 \oplus \Delta c_4 = 0. \end{aligned}$$

Therefore, the probability of a pair remains after this filtering is about 2^{-64}.

The third step of the attack is key recovery. First of all, for each guess of $(sk_{4,1}, sk_{4,2}, sk_{4,3})$ we can partially encrypt Round 4 to check if a pair satisfies the distinguisher. Note for each plaintext pair $X = (x_1, x_2, x_3, x_4)$ and $X^* = (x_1^*, x_2^*, x_3^*, x_4^*)$, a useful pair must satisfy that the output difference of the round

function in Round 4 equals to the input difference $x_4 \oplus x_4^*$. Therefore, based on this property we can discard some useless pairs to reduce the complexity in the following steps, and the probability of a pair remains after this filtering is about 2^{-21}. Then for all the remained pairs, we guess the values of rk_{25} and rk_{24} to decrypt Round 25 and Round 24 respectively. At last we recover the value of rk_{23} by differential techniques. Then we can discard all the wrong subkey guesses using the impossible differential sieving techniques.

In the following, we will describe the attack procedure in detail.

1. Data Collection: Choose 2^m structures and each structure is constructed as follows:
$$\begin{aligned} x_1 &= a_1, \\ x_2 &= a_2, \\ x_3 &= a_3, \\ x_4 &= (x_{4,1}, x_{4,2}, x_{4,3}, a_{4,4}), \end{aligned}$$
where (a_1, a_2, a_3) are 32-bit constants, $a_{4,4}$ is an 8-bit constant and the 3 bytes $(x_{4,1}, x_{4,2}, x_{4,3})$ take all the possible values of $(\{0,1\}^8)^3$. Then each structure contains 2^{24} plaintexts, which can generate about $2^{24} \cdot 2^{13}/2 = 2^{36}$ plaintext pairs. Therefore, 2^m structures can generate about 2^{m+36} plaintext pairs.
2. Data Filtering: According to the property of ciphertext difference, for a useful pair the difference $(\Delta c_1, \Delta c_2, \Delta c_3, \Delta c_4)$ should satisfy the following conditions.
$$\begin{aligned} \Delta c_1 &= 0, \\ \Delta c_1 \oplus \Delta c_2 \oplus \Delta c_3 \oplus \Delta c_4 &= 0. \end{aligned}$$
Therefore, after this test the expected number of remaining pairs is about $2^{m+36} \cdot 2^{-64} = 2^{m-28}$.
3. For each guess of the 24-bit subkey $(sk_{4,1}, sk_{4,2}, sk_{4,3})$, proceed as follows:
   (a) List all the possible values of rk_{23} as a table L.
   (b) For each of the remaining plaintext pair $X = (x_1, x_2, x_3, x_4)$ and $X^* = (x_1^*, x_2^*, x_3^*, x_4^*)$, partially encrypt Round 4 to compute the following values respectively.
$$\begin{aligned} \gamma &= (s(x_{4,1} \oplus sk_{4,1}) \oplus s(x_{4,1}^* \oplus sk_{4,1}), \quad s(x_{4,2} \oplus sk_{4,2}) \oplus s(x_{4,2}^* \oplus sk_{4,2}), \\ &\qquad s(x_{4,3} \oplus sk_{4,3}) \oplus s(x_{4,3}^* \oplus sk_{4,3}), \quad 0), \\ \lambda &= MDS^{-1}(x_4 \oplus x_4^*). \end{aligned}$$
   Then check if $\gamma = \lambda$ holds, and if this is not the case, discard the corresponding plaintext pair. After this test, there remains about $2^{m-28} \cdot 2^{-21} = 2^{m-49}$ plaintext pairs.
   (c) Guess the value of $rk_{25} = k_{26}^1 \oplus k_{26}^2 \oplus k_{26}^3 \oplus k_{26}^4$, and for each of the remaining pair, whose ciphertexts are denoted as (c_1, c_2, c_3, c_4) and $(c_1^*, c_2^*, c_3^*, c_4^*)$ respectively, do as follows.
      i. Compute the value of y_{25} as follows.
$$y_{25} = S^{-1}(MDS^{-1}(c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus rk_{25})).$$
      Note for the remaining pairs we have $\Delta y_{25} = 0$,
      and $y_{25}^* = S^{-1}(MDS^{-1}(c_1^* \oplus c_2^* \oplus c_3^* \oplus c_4^* \oplus rk_{25})) = y_{25}$.

ii. For each guess of the value $rk_{24} = sk_{25} \oplus k^1_{26} \oplus k^2_{26} \oplus k^3_{26}$, continue to compute the values of y_{24} and y^*_{24} as follows.

$$y_{24} = S^{-1}(MDS^{-1}(c_1 \oplus c_2 \oplus c_3 \oplus y_{25} \oplus rk_{24})),$$
$$y^*_{24} = S^{-1}(MDS^{-1}(c^*_1 \oplus c^*_2 \oplus c^*_3 \oplus y^*_{25} \oplus rk_{24})).$$

iii. If we denote the decryption function of Round 23 as $g(z, rk_{23}) = S^{-1}(MDS^{-1}(z \oplus rk_{23}))$, then for each remaining pair the inputs of g are $c_1 \oplus c_2 \oplus y_{24} \oplus y_{25}$ and $c^*_1 \oplus c^*_2 \oplus y^*_{24} \oplus y^*_{25}$ respectively, and the output difference of g should be $y_{24} \oplus y^*_{24}$. Therefore, by making use of the difference distribution table of Sbox we can compute the corresponding value of subkey rk_{23}. Discard it from the table L.

iv. If the table L is not empty after analyzing all the remaining pairs, we can output the value of rk_{23} remained in table L together with the corresponding guess of $(sk_{4,1}, sk_{4,2}, sk_{4,3})$, rk_{25} and rk_{24} as the correct subkey.

If we choose $m = 2^{87.5}$, then the number of useful pairs remained after the data filtering in Step 2 is about $2^{59.5}$. Hence there remains about $2^{38.5}$ pairs after the test of Step 3.b). In Step 3.c), according to the difference distribution table of Sbox, each pair can discard about one candidate of rk_{23}. Since there are 2^{32} possible values of rk_{23} in table L, then after analyzing all the $2^{38.5}$ remaining pairs, the probability of a subkey guess of rk_{23} still remains in L is about $(1 - 2^{-32})^{2^{38.5}} \approx e^{-2^{6.5}}$. Therefore, in Step 3.c.iv) the probability of a wrong subkey guess still remains after all the tests is about $2^{120} \times e^{-2^{6.5}} < 2^{-11}$, and this means that only the correct subkey will be output.

The data and time complexities of the attack can be estimated as follows. First of all, we choose $2^{87.5}$ structures which contains 2^{24} plaintexts each, and thus the data complexity of the attack is about $2^{24} \times 2^{87.5} = 2^{111.5}$ chosen plaintexts.

The time complexity of each step can be estimated roughly as follows. In Step 1, we need about $2^{111.5}$ encryptions. In Step 2 we have to check if the pair satisfies the ciphertext difference for all the $2^{123.5}$ pairs. Note the time needed for filtering is rather small which can be estimated as 2^{-3}-round encryption. Therefore, the time complexity of Step 2 is about $2^{123.5} \times \frac{1}{25} \times 2^{-3} < 2^{115.9}$ encryptions. In Step 3.b), we need to encrypt one round for each pair, which means that the time complexity is about $2^{24} \times 2^{59.5}/25 > 2^{78.9}$ encryptions. Similarly, the time complexities of Step 3.c.i) and Step 3.c.ii) are $2^{24} \times 2^{32} \times 2^{38.5} \times 1/25 < 2^{89.9}$ encryptions and $2^{24} \times 2^{32} \times 2^{32} \times 2^{38.5} \times 2/25 < 2^{122.9}$ encryptions respectively. In Step 3.c.iii), the operation to recover subkey rk_{23} from the difference distribution table of Sbox is rather simple and can be estimated as 1-round encryption. Then the time complexity of this step is about $2^{24} \times 2^{32} \times 2^{32} \times 2^{38.5} \times 1/25 < 2^{121.9}$ encryptions. Therefore, the total time complexity of the attack is less than $2^{123.5}$ encryptions.

5 Conclusion

In [29], Choy et al proposed a new structure called GF-NLFSR (Generalized Feistel-NonLinear Feedback Shift Register), and also examined the security of the structure against many attacks such as differential, linear, impossible differential and integral cryptanalysis. Furthermore, they designed a new block cipher called Four-Cell which is based on 4-cell GF-NLFSR structure. In this paper, we proved that for n-cell GF-NLFSR structure there exists $(n^2 + n - 2)$ rounds impossible differential. Then using this kind of 18-round impossible differential distinguisher together with some novel differential and impossible differential cryptanalysis techniques, we presented an impossible differential attack on the full 25-round Four-Cell. The data complexity of our attack is $2^{111.5}$ and the time complexity is less than $2^{123.5}$ encryptions. In addition, we expect the attack to be more efficient when the relations between different round subkeys can be exploited by taking the key scheduling algorithm into consideration.

Compared with the other kinds of generalized Feistel strucutres, the n-cell GF-NLFSR structure has some obvious advantage such as the ability of being parallel. However, if it is used to design a new block cipher, more work still need to be done about the security of the structure against various cryptanalysis and its pseudorandomness.

Acknowledgments. This work is supported by the National Natural Science Foundation of China (No.60873259), and the National High-Tech Research and Development 863 Plan of China (No.2007AA01Z470). Moreover, the authors are very grateful to the anonymous referees for their comments and editorial suggestions.

References

1. Nyberg, K., Kundsen, L.: Provable Security against Differential Cryptanalysis. Journal of Cryptology 1(8), 156–168 (1995)
2. Knudsen, L.: Practically secure Feistel ciphers. In: Anderson, R. (ed.) FSE 1993. LNCS, vol. 809, pp. 211–221. Springer, Heidelberg (1994)
3. Kanda, M.: Practical security evaluation against differential and linear cryptanalyses for feistel ciphers with SPN round function. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, p. 324. Springer, Heidelberg (2001)
4. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing 17(2), 373–386 (1988)
5. Lucks, S.: Faster Luby-Rackoff ciphers. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 189–203. Springer, Heidelberg (1996)
6. Patel, S., Ramzan, Z., Sundaram, G.: Towards making Luby-Rackoff ciphers optimal and practical. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 171–185. Springer, Heidelberg (1999)
7. Naor, M., Reingold, O.: On the construction of pseudorandom permutations Luby-Rackoff revisited. Journal of Cryptology 12(1), 9–66 (1999)
8. Maurer, U., Pietrzak, K.: The security of Many-Round Luby-Rackoff Pseudorandom Permutation. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 544–561. Springer, Heidelberg (2003)

9. Patarin, J.: Security of Random Feistel schemes with 5 or more rounds. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 106–122. Springer, Heidelberg (2004)
10. Wenling, W.: Pseudorandomness of Camellia-like scheme. Journal of Computer Science and Technology 12(1), 1–10 (2006)
11. Matsui, M.: New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 205–217. Springer, Heidelberg (1996)
12. Matsui, M.: New Block Encryption Algorithm MISTY. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997)
13. ETSI, Universal Mobile Telecommunications System (UMTS), Specification of the 3GPP confidentiality and integrity algorithms, Document 2: Kasumi specification (2007), http://www.etsi.org/website/document/algorithms/ts_135202v070000p.pdf
14. Iwata, T., Yoshino, T., Yuasa, T., Kurosawa, K.: Round security and super- pseudorandomness of MISTY type structure. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 233–247. Springer, Heidelberg (2002)
15. Piret, G., Quisquater, J.-J.: Security of the MISTY Structure in the Luby-Rackoff Model: Improved Results. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 100–115. Springer, Heidelberg (2004)
16. Kang, J.S., Yi, O., Hong, D., et al.: Pseudorandomness of Misty-type Transformations and the Block Cipher KASUMI. In: Varadharajan, V., Mu, Y. (eds.) ACISP 2001. LNCS, vol. 2119, pp. 60–73. Springer, Heidelberg (2001)
17. Iwata, T., Yagi, T., Kurosawa, K.: On the Pseudorandomness of KASUMI Type Permutations. In: Safavi-Naini, R., Seberry, J. (eds.) ACISP 2003. LNCS, vol. 2727, pp. 217–289. Springer, Heidelberg (2003)
18. Vaudenay, S.: On the Lai-Massey Scheme. In: Lam, K.-Y., Okamoto, E., Xing, C. (eds.) ASIACRYPT 1999. LNCS, vol. 1716, pp. 9–19. Springer, Heidelberg (1999)
19. Junod, P., Vaudenay, S.: FOX: a new Family of Block Ciphers. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 131–146. Springer, Heidelberg (2004)
20. Schneier, B., Kelsey, J.: Unbalanced Feistel Networks and Block Cipher Design. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 121–144. Springer, Heidelberg (2005)
21. Adams, C.: Constructing Symmetric Ciphers Using the CAST Design Procedure. Designs, Codes and Cryptography 12(3), 283–316 (1997)
22. MARS Block cipher, http://www.nist.gov/aes/
23. Specification of SMS4, Block Cipher for WLAN Products-SMS4 (in Chinese), http://www.oscca.gov.cn/UpFile/200621016423197990.pdf
24. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (Extended abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007)
25. 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)
26. Nyberg, K.: Generlized Feistel networks. In: Kim, K.-c., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 91–104. Springer, Heidelberg (1996)
27. Wu, W., Zhang, W., Lin, D.: On the Security of Generalized Feistel Scheme with SP Round Function. International Journal Network Security 2(3), 296–305 (2006)
28. Shirai, T., Shibutani, K.: On Feistel structures using a diffusion switching mechanism. In: Robshaw, M.J.B. (ed.) FSE 2006. LNCS, vol. 4047, pp. 41–56. Springer, Heidelberg (2006)

29. Choy, J., Chew, G., Khoo, K., Yap, H.: Cryptographic Properties and Application of a Generalized Unbalanced Feistel Network Structure. In: ACISP 2009. LNCS, vol. 5594, pp. 73–89. Springer, Heidelberg (2009)
30. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 12–23. Springer, Heidelberg (2003)
31. Phan, R.C.-W.: Impossible Differential Cryptanalysis of 7-round AES. Information Processing Letters 91(1), 33–38 (2004)
32. Zhang, W., Wu, W., Feng, D.: New Results on Impossible Differential Cryptanalysis of Reduced AES. In: Nam, K.-H., Rhee, G. (eds.) ICISC 2007. LNCS, vol. 4817, pp. 239–250. Springer, Heidelberg (2007)
33. Wu, W., Zhang, W., Feng, D.: Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia. Journal of Computer Science and Technology 22(3), 449–456 (2007)
34. Tsunoo, Y., Tsujihara, E., Shigeri, M., Saito, T., Suzaki, T., Kubo, H.: Impossible differential cryptanalysis of CLEFIA. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 398–411. Springer, Heidelberg (2008)
35. Dunkelman, O., Keller, N.: An Improved Impossible Differential Attack on MISTY1. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 441–454. Springer, Heidelberg (2008)
36. Kim, J.-S., Hong, S.H., Sung, J., Lee, S.-J., Lim, J.-I., Sung, S.H.: Impossible differential cryptanalysis for block cipher structures. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 82–96. Springer, Heidelberg (2003)