Information leakage of 1-Nested-Feistel network

Yao Cui¹, Xuchen Dong² and Hui Guan³,⁴
¹China Nuclear Power Engineering Company. Beijing, China, 100086
²China Nuclear Control Systems Engineering Co., Ltd. Beijing, China, 100000
³Information Science and Technology Institute. Zhengzhou, 450000, China
⁴Email: ciccr_ieu@126.com

Abstract. Impossible differential cryptanalysis is a powerful tool to evaluate the strength of a block cipher structure. In this paper, we investigate the impossible differential property of Nested-Feistel networks, which is a famous block cipher network used in lightweight block cipher design. We propose a 3-round 1-probability differential of 1-Nested-Feistel structures, which is a special case of Nested-Feistel network, by using this result, we can construct impossible differentials for any round of Nested-Feistel networks.

1. Introduction
Impossible differential cryptanalysis [1] was introduced by Biham to break the block cipher Skipjack [2], this is one of the most powerful attacks against block ciphers in last two decades and lots of research interests has been focus on this field. Impossible differential cryptanalysis has been used to attack Skipjack, Camellia, ARIA, n-cell etc. and got many wonderful results.

Since the powerful efficiencies of impossible differential cryptanalysis, many experts work on finding impossible differential distinguishers for block cipher structures [3]. In [4], Wei et al. provided several impossible differentials for classical Feistel ciphers. And in [5, 6], Li et al. proposed impossible differentials for SPN ciphers and MISTY ciphers.

The most sound block cipher structure is the Feistel structure [7-11], and in this paper, we will study the impossible differential property of 1-Nested-Feistel structure, which is a special case of Nested-Feistel structure, and this structure widely used in the design of some block cipher these days.

The paper is organized as below: Section 2 gives the definition of 1-Nested-Feistel structure and some basic concepts used throughout the paper. Section 3 gives our 3-round 1-probability differential on the 1-Nested-Feistel structure. Section 4 provides the impossible differential property of such network and Section 5 draws conclusion.

2. Preliminaries.
Throughout this paper, we will use ⊕ to denote the bitwise XOR operation, Δx denotes the XOR difference of x and x', Δf(Δx)' denotes the possible output difference of f when the given input difference is Δx.

Definition 1. Let S be a key-related bijection over \{0,1\}ⁿ, then the function NF, which satisfy

\[ NF(x₁, x₂, x₃, x₄) = (x₁ ⊕ x₂ ⊕ S(x₃), x₂ ⊕ x₄, x₃, x₄) \]

is called a 1-Nested-Feistel structure.
1-Nested-Feistel structure is a special case of the Nested-Feistel structure, for the latter, one of the most sound example is the block cipher DEAL.

**Definition 2.** Let \(f : \{0,1\}^n \rightarrow \{0,1\}^n\) and \(\alpha, \beta \in \{0,1\}^n\), the differential probability of \(f\) is defined by

\[
p_f(\alpha \rightarrow \beta) = \frac{1}{2^n} |\{x \in \{0,1\}^n : f(x \oplus \alpha) = f(x) \oplus \beta\}|.
\]

If \(p_f(\alpha \rightarrow \beta) = 0\), \(\alpha \rightarrow \beta\) is called an impossible differential.

It is widely known that if \(f\) is a bijection with \(p_f(\alpha \rightarrow \beta) > 0\), then \(\alpha \neq 0\) iff \(\beta \neq 0\).

**Theorem 1.** Let \((\Delta x_1, \Delta x_2, \Delta x_3, \Delta x_4) \rightarrow (\Delta y_1, \Delta y_2, \Delta y_3, \Delta y_4)\) be a differential of a single round Nested-Feistel structure, then we have

\[
\Delta y_1 = \Delta x_1 \oplus \Delta x_3 \oplus (\Delta_y(x_2)) \Delta y_2 = \Delta x_2 \oplus \Delta x_4, \Delta y_3 = \Delta x_1, \Delta y_4 = \Delta x_2
\]

**Proof.** Let \(X = (x_1, x_2, x_3, x_4)\) and \(X \oplus AX = (x_1, x_2, x_3, x_4) \oplus (\Delta x_1, \Delta x_2, \Delta x_3, \Delta x_4)\) be two of the input difference, then we take consider of the output difference of a single round Nested-Feistel structure as below,

\[
NF(X) \oplus NF(X \oplus AX)
\]

\[
= (x_1 \oplus x_3 \oplus S(x_2), x_2 \oplus x_4, x_1, x_2)
\]

\[
\oplus (x_1 \oplus \Delta x_1 \oplus x_3 \oplus \Delta x_3 \oplus S(x_2 \oplus \Delta x_2), x_2 \oplus \Delta x_2 \oplus x_4 \oplus \Delta x_4, x_1 \oplus \Delta x_1, x_2 \oplus \Delta x_2)
\]

\[
= (\Delta x_1 \oplus \Delta x_3 \oplus S(x_2) \oplus S(x_2 \oplus \Delta x_2), \Delta x_2 \oplus \Delta x_4, \Delta x_1, \Delta x_2)
\]

\[
= (\Delta x_1 \oplus \Delta x_3 \oplus (\Delta y(\Delta x_2)), \Delta x_2 \oplus \Delta x_4, \Delta x_1, \Delta x_2)
\]

Then we end the proof.

### 3. 1-probability differential property of 3-round 1-Nested-Feistel network

In this section, we will provide the proof of 3-round impossible differential property of Nested-Feistel network.

Before we start the main result, we will introduce the following property by using Theorem 1.

**Property 1.** Let \((\Delta x_1, \Delta x_2, \Delta x_3, \Delta x_4) \rightarrow (\Delta z_1, \Delta z_2, \Delta z_3, \Delta z_4)\) be a differential of \(r\)-round Nested-Feistel structure, if we have \(\Delta x_4 = 0\), then \(\Delta z_4 = 0\), furthermore, we can build some linear equations between invariants \(\Delta x_1, \Delta x_3, \Delta z_1, \Delta z_3\).

**Proof.** We start from a single round. Let \((\Delta x_1, 0, \Delta x_3, 0) \rightarrow (\Delta y_1, \Delta y_2, \Delta y_3, \Delta y_4)\) be a differential of a single round Nested-Feistel structure, then by Theorem 1, we have

\[
\Delta y_1 = \Delta x_1 \oplus \Delta x_3 \oplus (\Delta_y(x_2)) = \Delta x_1 \oplus \Delta x_3
\]

\[
\Delta y_2 = \Delta x_2 \oplus \Delta x_4 = 0
\]

\[
\Delta y_3 = \Delta x_1
\]

\[
\Delta y_4 = 0
\]

hold simultaneously. So the differential can be rewritten as \((\Delta x_1, 0, \Delta x_3, 0) \rightarrow (\Delta x_1 \oplus \Delta x_3, 0, \Delta x_1, 0)\).

By a simple mathematical deduction, we can conclude this property.

**Theorem 2.** Let \((\alpha, 0, \alpha, 0)\) be the input difference of 3-round 1-Nested-Feistel structure, then its output difference is always \((\alpha, 0, \alpha, 0)\).

**Proof.** By Theorem 1, if the input difference is \((\alpha, 0, \alpha, 0)\), then the output difference from round 1 to round 4 is listed as

- **Round 1.** \((0, 0, 0, 0)\), with probability 1, since the input difference of the unique nonlinear function \(S\) is 0.
- **Round 2.** \((\alpha, 0, 0, 0)\), with probability 1, since the input difference of the unique nonlinear function \(S\) is 0.
- **Round 3.** \((\alpha, 0, \alpha, 0)\), with probability 1, since the input difference of the unique nonlinear function \(S\) is 0.
By this Theorem, no matter how many round the 1-Nested-Feistel network cascade, there always exists information leakage.

Immediately, we may conclude the following Corollaries.

**Corollary 1.** (1) Let \((0,0,\alpha,0)\) be the input difference of 3-round 1-Nested-Feistel structure, then its output difference is always \((0,0,\alpha,0)\);
(2) Let \((\alpha,0,0,0)\) be the input difference of 3-round Nested-Feistel structure, then its output difference is always \((\alpha,0,0,0)\).

**Corollary 2.** (1) Let \((0,0,\alpha,0)\) be the input difference of 2-round 1-Nested-Feistel structure, then its output difference is always \((\alpha,0,0,0)\);
(2) Let \((\alpha,0,0,0)\) be the input difference of 2-round Nested-Feistel structure, then its output difference is always \((\alpha,0,0,0)\);
(3) Let \((\alpha,0,0,0)\) be the input difference of 2-round Nested-Feistel structure, then its output difference is always \((\alpha,0,0,0)\).

### 4. Impossible differential property of 1-Nested-Feistel network

Based on the 1-probability differential property, we can construct a mass of impossible differentials for such 1-Nested-Feistel network. The following Theorem is obviously.

**Theorem 3.** Let \(NF(r)\) be an \(r\)-round 1-Nested-Feistel network, then for any \(\alpha \in \{0,1\}^*\)
(1) if \(r \equiv 0 \mod 3\), then \((0,0,\alpha,0) \rightarrow \Delta_1\), \((\alpha,0,\alpha,0) \rightarrow \Delta_2\), and \((\alpha,0,0,0) \rightarrow \Delta_3\) are impossible differentials of \(NF(r)\);
(2) if \(r \equiv 1 \mod 3\), then \((0,0,\alpha,0) \rightarrow \Delta_1\), \((\alpha,0,\alpha,0) \rightarrow \Delta_3\), and \((\alpha,0,0,0) \rightarrow \Delta_2\) are impossible differentials of \(NF(r)\);
(3) if \(r \equiv 2 \mod 3\), then \((0,0,\alpha,0) \rightarrow \Delta_2\), \((\alpha,0,\alpha,0) \rightarrow \Delta_1\), and \((\alpha,0,0,0) \rightarrow \Delta_3\) are impossible differentials of \(NF(r)\).

where \(\Delta_i \in \{0,1\}^* \setminus \{0\}\), \(\Delta_2 \in \{0,1\}^* \setminus \{\alpha,0,0,0\}\), \(\Delta_1 \in \{0,1\}^* \setminus \{\alpha,0,0,0\}\).

**Example 1.** For 20-round 1-Nested-Feistel network, then for any \(\alpha,\beta \in \{0,1\}^*\), \((\alpha,0,\alpha,0) \rightarrow (\alpha,\beta,*,0)\) is an impossible differential, in which * means any value in the set \(\{0,1\}\).

We have noticed that this kind of impossible differentials may not lead an efficient differential attack or impossible differential attack, since differentials detected in this paper expose equal probability under any key. However, by applying this property, we can find efficient attack of this kind of cipher.

**Example 2.** For any integer \(r\), if a plaintext/ciphertext pair in \(3r\)-round 1-Nested-Feistel network is denoted by \((m_0, m_1, m_2, m_3)\) and \((c_0, c_1, c_2, c_3)\), then the plaintext of the ciphertext \((c_0 \oplus \alpha, c_1, c_2 \oplus \alpha, c_3)\) is \((m_0 \oplus \alpha, m_1, m_2 \oplus \alpha, m_3)\).

### 5. Conclusions

In this paper, we find differentials in 1-Nested-Feistel structure whose probability is 1. Since these differentials cannot distinguish the correct key from wrong ones, we failed in launching a key-recovery attack on this structure. However, this property causes a significant information leakage, and may lead to some weakness in special environments.

In spite of the weakness presented in this paper, Nested-Feistel structure retains some attractive features such as lightweight cost implementation and similarity in both decryption and encryption processes. However, the 1-round Feistel type round function is not a good choice, which makes our attacks succeed. A natural way to avoid such attack is to reinforce the round function, then the proof will be invalid for this case.

### References

[1] Knudsen L 1998 DEAL-A 128-bit Block Cipher. Technical Report 151 (Department of Informatics, University of Bergen, Bergen, Norway)

[2] Biham E, Biryukov A and Shamir A 1999 Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials (In: Stern, J. (ed.) EUROCRYPT LNCS Springer, Heidelberg)
1592 12-23

[3] Kim J, Hong S, Sung J, Lee S and Lim J 2003 Impossible Differential Cryptanalysis for Block Cipher Structures (In: Johansson, T., Maitra, S. (eds.) Indocrypt Springer, Heidelberg) 2904 82-96

[4] Wei Y, Li P, Sun B and Li C 2010 Impossible Differential Cryptanalysis on Feistel Ciphers with SP and SPS Round Functions (ACNS 2010, LNCS Springer-Verlag ) 6123 105-122

[5] Li R, Sun B and Li C 2010 Impossible differential cryptanalysis of SPN ciphers (Cryptology ePrint Archive http://eprint.iacr.org/2010/307)

[6] Li R, Sun B and Li C 2010 From Camellia to p-Camellia: Some Observations on MISTY Structure with SPN Round Function (Cryptology ePrint Archive http://eprint.iacr.org/2010/661)

[7] Cui T, Jin C and Huang K 2013 Information Leakage of VGF2 Structure (Mathematical Problems in Engineering https://www.hindawi.com/journals/mpe/2013/962342/)

[8] Wu W, Zhang W and Feng D 2007 Impossible differential cryptanalysis of reducedround ARIA and Camellia Journal of Computer Science and Technology 22(3) 449-456

[9] Sugita M, Kobara K and Imai H 2001 Security of reduced version of the block cipher Camellia against truncated and impossible differential cryptanalysis (In: Boyd, C. (ed.) ASIACRYPT Springer, Heidelberg) 2248 193-207

[10] Lu J 2007 Attacking reduced-round (versions of the SMS4 block cipher in the chinese WAPI standard ICICS’07, LNCS) 4861 306-318

[11] Tsunoo Y, Tsujihara E, Shigeri M, Saito T, Suzaki T and Kubo H 2008 Impossible Differential Cryptanalysis of CLEFIA (In FSE’08, LNCS Springer-Verlag) 398-411