Journal of Computer Virology and Hacking Techniques (2024) 20:295–300
https://doi.org/10.1007/s11416-023-00488-9

ORIGINAL PAPER

Full round impossible differentials for Feistel ciphers

D. Zakharov[1] · **M. Pudovkina**[1]

Received: 18 November 2022 / Accepted: 2 June 2023 / Published online: 24 June 2023
© The Author(s), under exclusive licence to Springer-Verlag France SAS, part of Springer Nature 2023

Abstract
In this paper a family of l round balanced Feistel ciphers with non-bijective functions F is being considered. For any such algorithm, the existence of impossible differentials for an arbitrary number of rounds l is proved. Construction method and lower bound of the number of such impossible differentials is obtained. The GRANULE cipher belongs to the family under consideration, for which a new approach for finding impossible differentials is proposed. Its superiority in comparison with other previously known approaches is shown both in terms of the number of impossible differentials found and in terms of the number of rounds. Experimental confirmation of the theoretical bound of the number of impossible differentials has been obtained.

Keywords Feistel cipher · Impossible differentials · Non-bijective function F · Impossible differentials search algorithm · GRANULE cipher

1 Introduction

Impossible differential cryptanalysis, independently proposed in [1] and [2], is one of the most common approaches for assessing the robustness of block ciphers.

Differential cryptanalysis was introduced by Eli Biham and Adi Shamir in [3] in late 1980s. The main idea of differential cryptanalysis is to consider differentials with relatively high probabilities and use them to distinguish the correct unknown keys from the wrong keys. When a correct key is used to decrypt the last few rounds of big number of pairs of ciphertexts, it is expected that the difference predicted by the differential appears more frequently, while when a wrong key is used the difference occurs less frequently.

In contrast, in the new variant of differential cryptanalysis particular differences that should not occur (i.e. that their probability is exactly zero) are predicted by differential, and thus a pair of ciphertexts can never be decrypted to that difference with the correct key. Therefore, if a pair is decrypted to this difference under some trial key, then certainly this trial key is not the correct one. This is a sieving attack which finds the correct keys by eliminating all the other keys which lead to contradictions. The differentials with probability zero are commonly called impossible differentials, and the method that uses such differentials is known as impossible differentials cryptanalysis. Cryptanalysis with impossible differentials is very powerful against many ciphers with various structures.

For example, it was used to analyze such block ciphers as Skipjack [1], DEAL [2], Present [4], CLEFIA [5], Simon [5], Camellia [5], Lblock [5] and AES [6], as well as to analyze structures commonly used in block cipher construction: XSL [7], Feistel network [8] and its generalizations [9].

Differential is commonly defined as a pair of plaintexts and ciphertexts differences (ϵ, δ). In case of differential cryptanalysis this means that a pair of plaintexts with fixed difference ϵ is more likely to be encrypted into pair of ciphertexts with difference δ after the number of rounds defined by the differential. Impossible differential, on the other hand, means that no matter what plaintexts pair with fixed difference ϵ will be encrypted not a single pair of ciphertext with a difference δ and after a number of rounds according to differential will be obtained.

A technique named miss-in-the-middle is often used to find impossible differentials. The idea behind this technique is quite simple: to find an $(m+d)$ round differential we need to find such (ϵ, δ) that $\epsilon \rightarrow \alpha$ after m rounds of encryption and $\beta \leftarrow \delta$ after d rounds of decryption and α and β somehow contradict each other. By $\epsilon \rightarrow \alpha$ we understand a process of difference encryption. It is not obvious how a

✉ D. Zakharov
zakhar343@yandex.ru

[1] National Nuclear Research University (Moscow Engineering-Physics Institute), Moscow, Russia

non-linear transformation affects the difference, but a common technique is to introduce a new variable for every bit of a non-zero sub-block of the output difference. In some cases, more information can be obtained for the output difference, but it depends on the specific properties of the S-box. In this paper we follow the common approach.

Impossible differentials can be used in distinguishing [9], [10] or key recovering [5], [6] attacks. The search for such differentials for the largest number of rounds possible is the main task behind impossible differentials attack.

In this paper a family of l round balanced Feistel ciphers with non-bijective functions F is considered. For each of them, the existence of impossible differentials for an arbitrary number of rounds l is proved, and a lower bound of the number of described impossible differences $3 \times 2^{(2n-2)}$ is obtained, where n is the length of the data block. The GRANULE [11] cipher relates to the family under consideration. A new approach for finding GRANULE impossible differentials is proposed. Its superiority in comparison with other previously known approaches [10] is shown both with respect to the number of impossible differentials found (144) and the number of rounds (7). Experimental confirmation of the theoretical bound of the number of impossible differentials is obtained.

The paper is organized as follows: descriptions of a family of balanced Feistel ciphers with a non-bijective function F and GRANULE cipher are given in Sect. 2. A theorem on lower bound of the number of impossible differentials for a family of algorithms under consideration is presented in Sect. 3. In Sect. 4 we propose a new algorithm for finding impossible differentials for GRANULE cipher.

2 A family of balanced Feistel ciphers

In this paper we consider a family of iterated block ciphers with $l > 3$ rounds of Feistel permutations and $n = 2m$ bits block size. The outline of a cipher is given in Fig. 1, where rk_i are round keys and function F is a composition of $h^{(0)}$ and $h^{(1)}$ transformations. We will call this family NBF and particular member of the family $NBF(A, n)$, where A is a

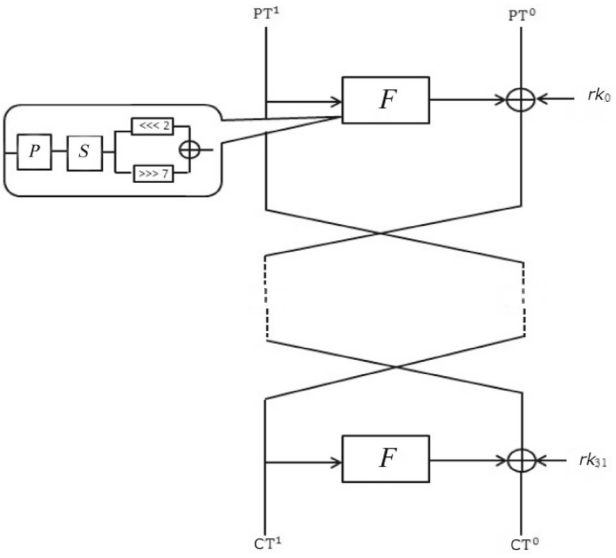


Fig. 2 GRANULE cipher outline [11]

$m \times m$ boolean matrix that defines the $h^{(1)}$ linear transformation and n is the block size as mentioned above.

No restrictions are imposed on $h^{(0)}$ mapping, but $h^{(1)}$ must be a linear transformation with its matrix rank equal to $m - 1$.

A balanced Feistel based cipher with 32 rounds of encryption GRANULE [11] can be cited as a member of a family of ciphers under consideration. The block size equals to 64 bits, and the key size equals to 80 or 128 bits, round key has a size of 32 bits. Figure 2 [11] shows the outline of the GRANULE cipher.

GRANULE function F can be viewed as a composition of a linear layer, an S-box layer and a linear layer, which includes two cyclic shift operations and an addition operation modulo 2. In the first linear layer, a 32-bit vector is divided into 8 sub-blocks of 4 bits, then these sub-blocks are rearranged in accordance with the permutation presented in Table 1 [11]. We denote the function of this layer as P.

After a linear layer operation is performed an S-box mapping is applied to every 4 bit block. GRANULE S-box is presented in Table 2 [11].

The last layer of function F combines application of cyclic shift and exclusive-or operations. We denote the function of

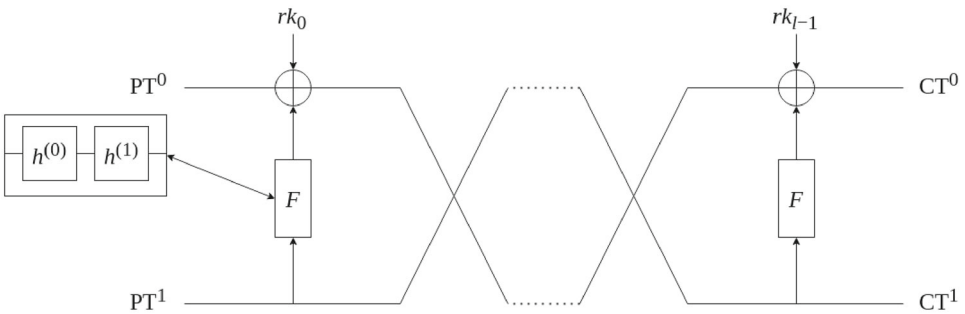


Fig. 1 Outline of the family of ciphers under consideration

Table 1 Permutation layer of GRANULE

x	0	1	2	3	4	5	6	7
$P[x]$	4	0	3	1	6	2	7	5

Table 2 S-box of GRANULE

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	e	7	8	4	1	9	2	f	5	a	b	0	6	c	d	3

this layer as RP and it can be defined as

$$OUT \leftarrow (IN <<< 2) \oplus (IN >>> 7),$$

where IN is the input m bit boolean vector and OUT is the output m bit boolean vector of this layer. In other words, $OUT = RP(IN)$.

Key schedule algorithm of the GRANULE cipher is presented below:

$$\begin{aligned}
&k <<< 31,\\
&[k_3k_2k_1k_0] \leftarrow S[k_3k_2k_1k_0],\\
&[k_7k_6k_5k_4] \leftarrow S[k_7k_6k_5k_4],\\
&[k_{70}k_{69}k_{68}k_{67}k_{66}] \leftarrow [k_{70}k_{69}k_{68}k_{67}k_{66}] \oplus [i]^2,
\end{aligned}$$

where k is the encryption key and k_i is the i-th bit of k, S is the S-box, and $[i]^2$ is a binary representation of a decimal number i.

3 Full round impossible differentials for the *NBF* ciphers

In this section, for any NBF cipher a method for constructing impossible differentials for an arbitrary number of rounds is proposed, and a theoretical bound of the number of such differentials is given. The method does not depend on the bijective part $h^{(0)}$ of function F, nor on the key schedule algorithm.

Definition 1 We will call an impossible differential (ϵ, δ) trivial if $\epsilon = 0$ or $\delta = 0$.

Theorem 1 *Any $NBF(A, n)$ cipher $(rank(A) = m-1, n = 2m)$ has at least $3 \times 2^{2n-2} - 2^{n+1}$ full round impossible nontrivial differentials.*

Proof To construct the differentials, we will use the miss-in-the-middle technique. We will denote Ω as an image of function F, so that

$$\Omega = \{F(\beta) | \beta \in \{0, 1\}^m\}.$$

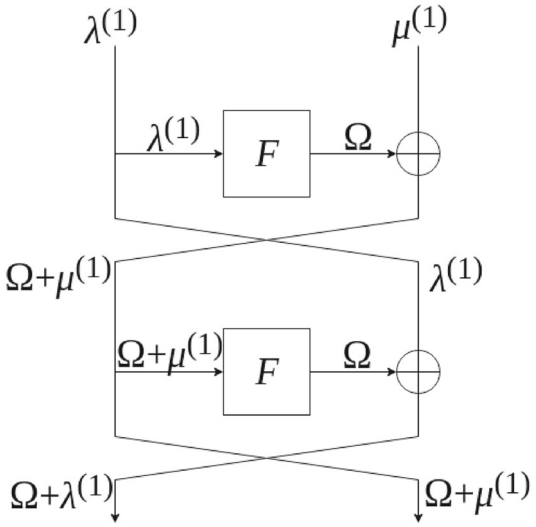


Fig. 3 Encryption of $(\lambda^{(1)}, \mu^{(1)})$ differences by 2 rounds

Fig. 3 shows an encryption outline of $\epsilon = (\lambda^{(1)}, \mu^{(1)})$ by 2 rounds.

Similarly, the $\delta = (\lambda^{(2)}, \mu^{(2)})$ is decrypted to $(\Omega + \lambda^{(2)}, \Omega + \mu^{(2)})$ after 2 rounds. For (ϵ, δ) to be an impossible even number of rounds differentials $(\Omega + \lambda^{(1)}, \Omega + \mu^{(1)})$ and $(\Omega + \lambda^{(2)}, \Omega + \mu^{(2)})$ must somehow contradict each other.

Let us consider $\Omega + \lambda^{(1)}$ and $\Omega + \lambda^{(2)}$. Since $rank(A) = m - 1$ there is always a set of d indexes $\{i_1, ..., i_d\}$ such that the relation

$$\sum_{j=1}^{d} \omega_{i_j} \equiv 0 \pmod 2$$

holds for each $\omega \in \Omega$, but if

$$\sum_{j=1}^{d} \lambda_{i_j}^{(1)} \not\equiv \sum_{j=1}^{d} \lambda_{i_j}^{(2)} \pmod 2$$

we get the required contradiction. It is important to note, that from the property above we get that $\Omega + \Omega = \Omega$.

The number of found impossible differentials can be estimated as

$$2^{2n} - (2^m \times 2^{m-d} \times 2^{d-1})^2 = 2^{2n} - 2^{2n-2} = 3 \times 2^{2n-2},$$

where the number of trivial impossible differentials can be estimated as

$$2^n \times 2 = 2^{n+1}.$$

Here 2^{2n} is the total number of n-bit differentials. $(\Omega + \lambda^{(1)}, \Omega + \mu^{(1)})$ and $(\Omega + \lambda^{(2)}, \Omega + \mu^{(2)})$ contradict each other in any case other than $(\Omega + \lambda^{(1)}) \cap (\Omega + \lambda^{(2)}) \neq \emptyset$ and

$(\Omega+\mu^{(1)})\cap(\Omega+\mu^{(2)}) \neq \emptyset$. $2^m \times 2^{m-d} \times 2^{d-1}$ is the number of differentials, that satisfy the condition $(\Omega + \lambda^{(1)}) \cap (\Omega + \lambda^{(2)}) = \emptyset$ or the condition $(\Omega + \mu^{(1)}) \cap (\Omega + \mu^{(2)}) = \emptyset$. For the first set we can pick any difference we want, thus we have 2^m possible vectors. For the second set we can choose any $m-d$ bits, but from remaining d bit we must choose one to satisfy the condition above.

It is important to note that after even number of rounds $\epsilon = (\lambda^{(1)}, \mu^{(1)})$ will be encrypted into $(\Omega + \lambda^{(1)}, \Omega + \mu^{(1)})$, but after odd number of rounds ϵ will be encrypted to $(\Omega + \mu^{(1)}, \Omega + \lambda^{(1)})$. Thus for (ϵ, δ) to be an impossible odd number of rounds differentials $(\Omega + \mu^{(1)}, \Omega + \lambda^{(1)})$ and $(\Omega + \lambda^{(2)}, \Omega + \mu^{(2)})$ must somehow contradict each other. We have come to the same condition as in the case of an even number of rounds, so the theorem is also fulfilled for an odd number of rounds □

Note that Theorem 1 imposes restrictions exclusively on the last linear layer of the function F, hence the obtained result does not depend on its bijective part, including the S-box layer.

Also note that from the definition of the rank of the matrix there are $m - rank(A)$ sets of indexes $\{i_1, ..., i_d\}$ that satisfy the condition

$$\sum_{j=1}^{d} \omega_{i_j} \equiv 0 \pmod 2.$$

If $rank(A) < m-1$ many more impossible differentials can be constructed.

It was shown that GRANULE cipher belongs to family defined in Section 2, therefore GRANULE has at least $3 \times 2^{126} - 2^{65}$ nontrivial impossible differentials for an arbitrary number of rounds. For comparison, an automated search for GRANULE impossible differentials was performed in [10] and only 144 impossible 7-round differentials were found (only such $(\epsilon, \delta) \in \{0,1\}^n \times \{0,1\}^n$, that $\|\epsilon\| = \|\delta\| = 1$ were considered in [10]). It is worth noting that some differentials found in [10] do not meet the criterions of Theorem 1.

4 GRANULE impossible differentials search algorithm

The search algorithm proposed in [10] does not take into account the irreversibility of the GRANULE function F. Any 4 bit input difference is transformed by the S-box into 4 unknown and more importantly indistinguishable bits "****", thus the $h^{(1)}$ property discussed in Sect. 3 is not used.

Algorithm 1 Performs difference encryption by 1 round

Require: l, r arrays and round number i
Ensure: l, r arrays
1: $l \leftarrow P(l)$
2: **for** $j = 0$ to 7 **do**
3: **if** $l[j] \neq 0000$ **then**
4: $l[j] \leftarrow \alpha^i_{4j}\alpha^i_{4j+1}\alpha^i_{4j+2}\alpha^i_{4j+3}$
5: **end if**
6: **end for**
7: $l \leftarrow RP(l)$
8: **return** $r \oplus l, l$

Algorithm 2 Finds n round impossible differential

Require: number of rounds n
Ensure: n-round impossible differentials
1: **for** $upper_block$ in $4bit_blocks$ **do**
2: **for** $lower_block$ in $4bit_blocks$ **do**
3: **for** $upper_block_pos = 0$ to 7 **do**
4: **for** $lower_block_pos = 0$ to 7 **do**
5: **for** $down = 1$ to $[\frac{n}{2}]$ **do**
6: $l, r \leftarrow init()$ ▷ Initialize l, r with 8 "0000" 4 bit blocks
7: $r[upper_block_pos] \leftarrow upper_block$
8: **for** $i = 1$ to $down$ **do**
9: $l, r \leftarrow encrypt(l, r, i)$ ▷ Algorithm 1
10: **end for**
11: $down_l, down_r \leftarrow l, r$
12: $l, r \leftarrow init()$ ▷ Initialize l, r with 8 "0000" 4 bit blocks
13: $r[lower_block_pos] \leftarrow lower_block$
14: **for** $i = n$ downto $n - down$ **do**
15: $l, r \leftarrow encrypt(l, r, i)$ ▷ Algorithm 1
16: **end for**
17: $up_l, up_r \leftarrow r, l$ ▷ Decryption, so swap l, r
18: $eq_sys \leftarrow equalize(down_l \| down_r, up_l \| up_r)$
19: **if** $!is_solvable(eq_sys)$ **then**
20: $print(down_l + down_r, up_l + up_r)$
21: $break$ ▷ Found n round impossible differential
22: **end if**
23: **end for**
24: **end for**
25: **end for**
26: **end for**
27: **end for**

The main idea of our method is to use uniquely named variables when denoting the output difference bits of the S-box layer, as it was proposed in [10].

Obviously, since the nonlinear operation was replaced, then after an arbitrary number of rounds, each bit of the output difference is a linear polynomial. We use the miss-in-the-middle technique, and if the system of equations obtained after equating the decrypted and encrypted differences has no solution, then impossible differential is found.

The algorithm searches for n round (any m, d such that $n = m + d$) impossible differentials and can be divided into two parts: Algorithm 1 and Algorithm 2. Algorithm 1 is an internal part of the Algorithm 2 and implements encryption for 1 round of the input difference. A detailed description

Table 3 Computational experiment results

Number of rounds of the differential	Number of nontrivial impossible differentials	Execution time (in seconds)
4	14288	1.681
5	14288	1.751
6	13216	3.241
7	13216	3.332
8	7168	4.002
9	7168	4.082
10	7168	4.659
13	7168	5.511
16	7168	6.909
19	7168	7.746
22	7168	9.107
25	7168	9.975

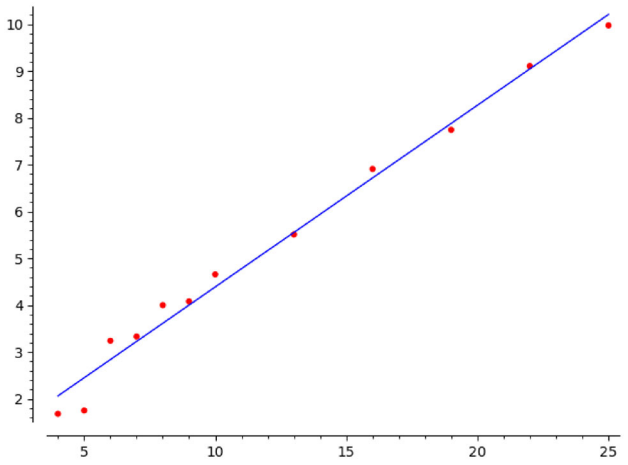


Fig. 4 Dependency of the execution time (sec.) on number of rounds of the differential

of the Algorithm 1 is provided below. The description of functions P and RP can be found in Section 2.

Algorithm 2 searches for all n round impossible differentials where both plaintext and ciphertext differences, $\Delta T = L \| R$, $L = 0$ and R includes the only nonzero 4 bit sub-block. The list of 4 bit sub-blocks consists of all possible 4 bit words. A detailed description of the Algorithm 2 is provided below.

The $equalize$ function in Algorithm 2 produces a linear system of equations by coordinate addition modulo 2 of the input differences. The $is_solvable$ function calculates the rank of the linear system matrices (system matrix and extended matrix) and determines wether this system of equations is solvable or not.

This algorithm was implemented in Python programming language. The computational experiment was held on Debian 12 system with Intel 12100f processor in order to estimate the asymptotic complexity of the algorithm. The results of the experiment are presented in Table 3, execution time is the average of 100 runs.

Figure 4 proves linear dependency of the execution time on the number of rounds of the differential ($y = kx + b$; $k \approx 0.388$, $b \approx 0.511$). We used SageMath $find_fit$ method to calculate parameters k, b.

Thus the asymptotic complexity of this algorithm can be estimated as $O(l)$, where l is the number of rounds of the differential.

For $l > 7$ the number of found nontrivial impossible differentials remains constant and equals to $8 \times 8 \times 7 \times 8 \times 2 = 7168$. We repeated the search for every $l > 7$ and $l < 26$, but discarded all the differentials that satisfied the theorem 1. This resulted in 0 found differentials.

It is of great interest to compare the most recent search results for impossible differentials to our results. In [10] study authors were able to find 144 7-round impossible differentials. Despite the fact that the list of found differentials is only partially given, we note that they found both differentials satisfying the condition of Theorem 1 and not satisfying. In our study we were able to find 7168 differentials, that satisfy conditions of Theorem 1 and 6048 differentials, that do not satisfy this conditions for 7 rounds of encryption.

It is important to note, that Theorem 1 differentials cannot be used to attack a cipher using impossible differentials attack, or at least cannot be use to sieve wrong keys. No matter how many rounds it takes to decrypt α to α' and to encrypt β to β', if (α, β) is a Theorem 1 impossible differential, then (α', β') is also an impossible differential.

5 Conclusions

In this study we introduced a family of balanced Feistel ciphers with non-bijective functions F for which an existance of impossible differentials for an arbitrary number of rounds was proved. Lower bound of the number of such differentials was obtained.

We also proposed a new method for automated impossible differentials search, that allowed us to get the best known result with respect to the number of differentials found for 7-round GRANULE cipher, that is a member of the family mentioned above.

We showed, that only certain impossible differentials can be used as distinguishers in impossible differentials attack, but only those, that do not spread on an arbitrary number of rounds.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

References

1. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Advances in Cryptology–EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18. Springer. (1999), pp. 12–23
2. Knudsen, L.: DEAL-a 128-bit block cipher. In: complexity 258.2, p. 216 (1998)
3. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard, 9th edn., p. 188. Springer, New York (1993)
4. Tezcan, C.: Improbable differential attacks on present using undisturbed bits. J. Comput. Appl. Math. **259**, 503–511 (2014)
5. Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon. In: Advances in Cryptology-ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, ROC, December 7-11, 2014. Proceedings, Part I 20. Springer. pp. 179–199 (2014)
6. Phan, Raphael C.-W.: Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES). In: Information processing letters 91.1, pp. 33–38 (2004)
7. Li, R., Sun, B., Li, C.: Impossible differential cryptanalysis of SPN ciphers. IET Inf. Secur. **52**, 111–120 (2011)
8. Wei, Y. et al.: Impossible differential cryptanalysis on Feistel ciphers with SP and SPS round functions. In: Applied Cryptography and Network Security: 8th International Conference, ACNS 2010, Beijing, China, June 22-25, 2010. Proceedings 8. Springer. pp. 105–122 (2010)
9. Cui, T., Jin, C., Ma, J.: A new method for finding impossible differentials of generalized Feistel structures. Chin. J. Electron. **27**(4), 728–733 (2018)
10. Xiaonian, W.U., et al.: Analysis of impossible differential distinguisher for GRANULE and MANTRA ciphers. J. Commun. **41**, 94–101 (2020)
11. Bansod, G., Patil, A., Pisharoty, N.: GRANULE: an ultra lightweight cipher design for embedded security. In: Cryptology ePrint Archive (2018)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.