On the Security of Extended Generalized Feistel Networks

Manoj Kumar*[1], Saibal K. Pal [1] & Anupama Panigrahi [2]
*mktalyan@yahoo.com**
SAG, DRDO, Metcalfe House, Delhi, INDIA[1]
Department of Mathematics, University of Delhi, Delhi, INDIA[2]

Abstract: In this paper, we analyze the security claims of Extended Generalized Feistel Networks (EGFNs) schemes proposed by Berger et al [1]. We provide impossible differentials for 10 rounds of EGFNs with 16 branches which add up one round to the claim of 9 rounds in the impossible differential trail. Therefore, impossible differential trail covers 10 rounds for the EGFNs scheme, which is the best result on impossible differentials of EGFNs so far. We also provide several 10 round impossible differential trails to attack EGFNs based new cipher proposals. $\mathcal{U}$–method is also used by authors to assert their claim for maximum number of rounds in impossible differential trails of EGFNs. This analysis indicates that $\mathcal{U}$–method does not provide optimal results for this scheme.

Keywords: Feistel Network, Generalized Feistel Network, Impossible Differential Cryptanalysis, $\mathcal{U}$–method

1. Introduction:

Feistel networks [2] are the extensively studied structures among the cryptographic primitives as compared to the Substitution Permutation Networks (SPN) [5] and other structures. Feistel networks have been used widely as a base structure in the designs of a large number of cryptographic primitives including Data Encryption Standard (DES) [10]. The first application of Feistel network is found in the design of block cipher Lucifer [13] which was designed by Horst Feistel himself and later modified to be accepted as DES. Several generalizations of Feistel networks and their analysis [4][6][8][12][14] have also been published in the literature and applied in the new block cipher proposals. EGFNs have been proposed as a new class of generalized Feistel schemes for cryptographic applications.

The classical Feistel network processes the data by dividing the block length n into two equal parts: b_1 and b_2. Several generalizations of Feistel networks are proposed by increasing the number of divisions of the block length n from 2 parts to k parts: $b_1, b_2, \ldots b_k$. The block length n may be divided into k equal or unequal parts. The unequal division [12][15] of block length has not gained much attention of designers and it is not used in practice for designing new cryptographic primitives. The division of block is mostly done into k equal parts and these k divisions are mostly multiples of 2. The Feistel and generalized Feistel networks (GFN) with such divisions are called balanced Feistel and balanced GFN with k branches. Block cipher designs based on GFN proposed in the literature are mostly 4-branch GFNs. Several studies on the 4-branch GFNs have been published and the categorization of 4-branch GFN is done in 4 ways: type I, type II, type III and type IV [4]. This categorization is basically done on the basis of number of round functions used and the number of Feistel branches remaining unchanged for the next round.

Our Contributions: We have applied impossible differential attack on the particular scheme of EGFNs with 16 branches, 64-bit block size and diffusion delay $d=4$ (the minimum number of rounds in which the full diffusion is achieved) as proposed in SAC 2013 by Berger et al. It was claimed by authors that maximum number of rounds covered in impossible differential trail is $2d+1$ for this scheme. $\mathcal{U}$-method is used to provide accurate estimates for the maximum number of rounds in the impossible differential trails of block ciphers [7][9]. Authors have also supported their claim with the results obtained using $\mathcal{U}$-method. For $d=4$, the maximum number of rounds in the trail is claimed to be *9* in [1]. We have increased this number by *1* and asserted that the number of rounds in the impossible differential trail of these EGFNs is 10. We provide several 10-round impossible differential trails for EGFNs which can be used to mount impossible differential attack on EGFN based schemes for more number of rounds.

Organization of the rest part of the paper is as follows. We describe a particular example of 16-branch EGFN schemes in the second section. We describe the impossible differential attack on this scheme in third section with detailed method for finding impossible differential trail for 10 rounds. Fourth section discusses the impact of this analysis on other proposals relying on the security estimates provided by $\mathcal{U}$-method with further work and finally conclude the paper.

2. Extended Generalized Feistel Networks (EGFNs):

Berger et al proposed the EGFNs using Matrix representation [1] with the security estimates in SAC 2013. Several properties of GFN layer are presented by authors representing these as matrix $M = P \text{ x } F$, where P is used for permutation layer and F is used for round functions. GFN are investigated exhaustively with 8 blocks for various parameters like the full diffusion delay d in [1], the number of round functions N_f used in each round and the cost for achieving full diffusion C_{fd}. It was reported in [1] that no GFN exist with cost C_{fd} less than 24 and the minimum number of round functions required for full diffusion in 6 rounds is 4. Authors extended this analysis and presented the Extended GFNs to achieve full diffusion in fewer rounds and less round functions. An efficient example of this EGFNs scheme (Fig. 1) presented in [1] is discussed below in detail. This EGFNs scheme can be used to design a lightweight block cipher with block size 64-bit or a block cipher with bigger sizes like 128, 192 and 256 bits. The only non-linear part of this scheme is the round function. An immediate application of this EGFN scheme will be a new lightweight block cipher with 64-bit block size and 4-bit S-box used in round function. The design may consist of three layers as key addition layer, S-box layer and the permutation layer.

2.1 EGFNs with 64-bit block size and 16 branches

Input and output block size of EGFNs scheme is 64-bit which is divided into 16 equal parts X_i's and Y_i's respectively. Each round consists of non-linear function, XOR operation and nibble permutation. The only non-linear function used in these 16 branch EGFNs is 4-bit S-box which takes 4-bit input and outputs 4-bit as described below:

Input: $X = (X_0, X_1, \ldots X_{15})$

Output: $Y = (Y_0, Y_1, \ldots Y_{15})$

$Y_0 = X_8 \oplus S(X_7)$

$Y_i = X_{8+i} \oplus X_7 \oplus S(X_{7-i});\ 1 \leq i \leq 6$

$Y_7 = (X_{15} \oplus X_7 \oplus X_6 \oplus \ldots\ldots \oplus X_1) \oplus S(X_0)$

$Y_i = X_{i-8};\ 8 \leq i \leq 15$

Table 1: Extended GFNs with 16 branches

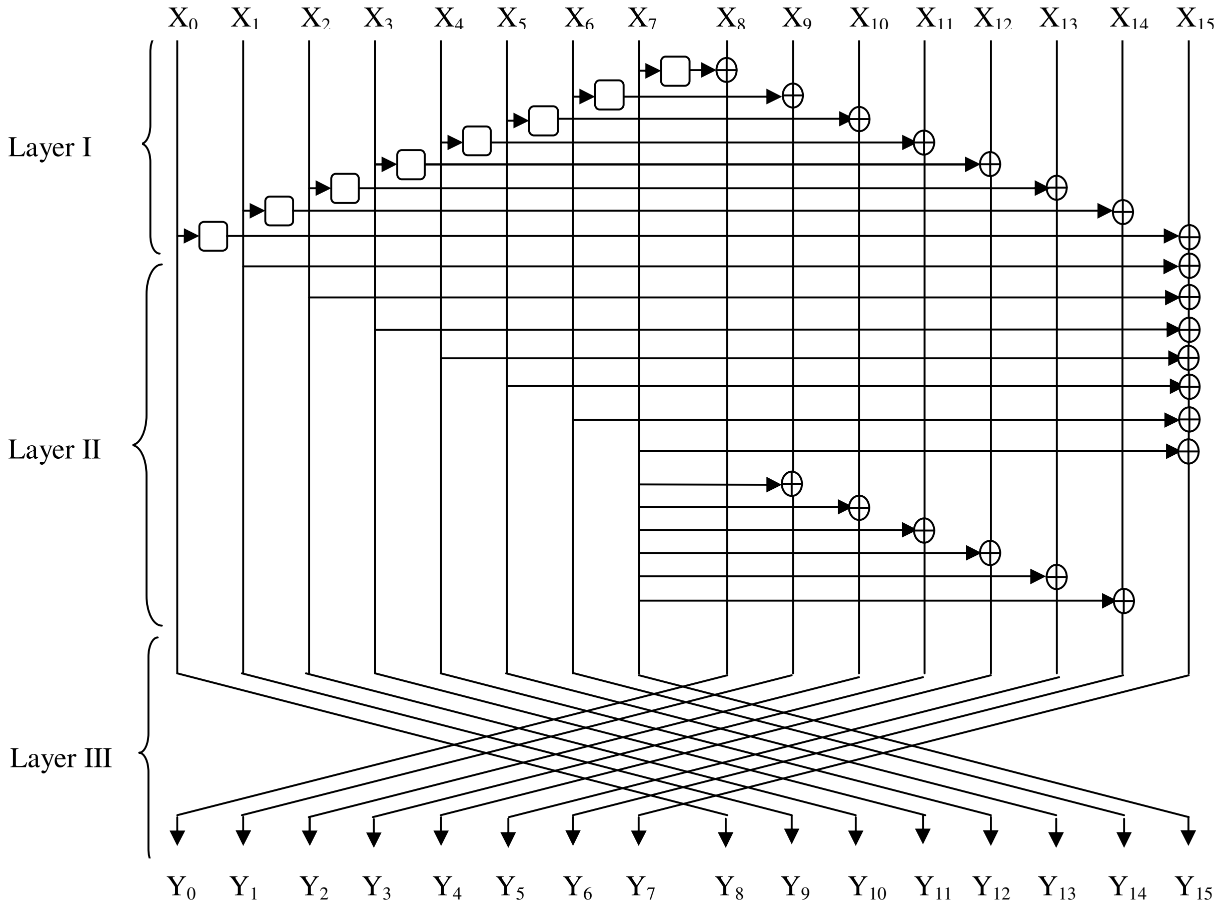

Fig. 1: EGFNs Example with 16 branches

3. Impossible Differential Cryptanalysis of EGFN:

Impossible differential cryptanalysis [3] is an extension of differential cryptanalysis which was applied by Biham et al. We work with zero probability differentials in this attack rather than working with high probability differences in differential attack. It is the best cryptanalysis method in terms of covering the most number of rounds for majority of the block cipher designs, one of the examples being the Advanced Encryption Standard (AES) [5]. This attack is proven to be more effective in practice than other attacks and it is necessary for all the new cipher proposals to show the resistance to this attack. The zero probability differentials are used to find out the correct key by sieving all the keys suggesting the impossible differential and the correct one still surviving in the list. The impossible differential trail is usually constructed using miss-in-the-middle approach [3] which finds trail by showing a contradiction between two differentials of probability 1. We construct probability 1 differential for some *r* forward rounds and also for some *s* backward rounds. If this probability 1 differentials show some disagreements at some intermediate level, then we have constructed an impossible differential trail for the total *r+s* rounds.

Differential cryptanalysis of EGFNs, presented by Zhang et al [16] has also improved the security estimates given by authors for differential cryptanalysis. We investigated the security claims of EGFNs scheme for impossible differential attack. We found that the number of rounds calculated in impossible differential trail can be improved further from the author's claim. The maximum number of rounds in the impossible trail given by the authors is 9 for diffusion delay *d=4* and the claim is supported by showing the same results from $\mathcal{U}$-method [7][9]. We provide several impossible differential trails for 10 rounds of EGFNs in this paper. This analysis will work irrespective of the block size of EGFNs as the non-linearity of round function is considered in this analysis. We discuss the method for finding the 10 round impossible differential trail below and provide several trails for 10 rounds in table 3.

3.1 EGFNs algorithm in forward direction

We rewrite the algorithm for 16 branch EGFNs described in Table 1 for input and output values $X_0, X_1,\ldots, X_{15}$ and $Y_0, Y_1,\ldots, Y_{15}$ respectively by dividing it into three layers viz. I, II and III for analysis purpose:

```
Layer I:     for i= 0 to 7, $U_i = X_i$;
             for i=8 to 15, $U_i = X_i \oplus S(X_{15-i})$
Layer II:    for i= 0 to 8, $V_i = U_i$;
             for i=9 to 14, $V_i = U_7 \oplus U_i$;
             for i=15, $V_i = U_1 \oplus U_2 \oplus U_3 \oplus U_4 \oplus U_5 \oplus U_6 \oplus U_7 \oplus U_{15}$
Layer III:   for i=0 to 15, $Y_i = V_{(8+i)\%16}$
```

3.2 EGFNs algorithm in backward direction

For the backward direction, we consider $Y_0, Y_1,\ldots, Y_{15}$ as input and $X_0, X_1,\ldots, X_{15}$ as output. Accordingly we rewrite the algorithm described in table 1 for input and output branches in backward direction as follows:

```
Layer III:   for i=0 to 15, $U_i = Y_{(8+i)\%16}$
Layer II:    for i= 0 to 8, $V_i = U_i$;
             for i=9 to 14, $V_i = U_7 \oplus U_i$;
             for i=15, $V_i = U_1 \oplus U_2 \oplus U_3 \oplus U_4 \oplus U_5 \oplus U_6 \oplus U_7 \oplus U_{15}$
Layer I:     for i= 0 to 7, $X_i = V_i$;
             for i=8 to 15, $X_i = V_i \oplus S(V_{15-i})$
```

3.3 Impossible Differential Trail for 10 rounds of EGFNs

We start with 16 branches each as input and output to this EGFNs example labeled as $X_0, X_1, \ldots, X_{15}$ and $Y_0, Y_1, \ldots, Y_{15}$ respectively. We assign some non-zero value α to one of the 16 branches. After one application of S-box on α, we get β which is also some non-zero value by the property of difference distribution table of S-boxes. Once again we apply S-box on β gives us some non-zero value γ and finally we get some non-zero value δ by applying S-box on γ one more time. This process can be represented as follows:

$$S(\alpha) = \beta,\ S(S(\alpha)) = S(\beta) = \gamma,\ S(S(S(\alpha))) = S(S(\beta)) = S(\gamma) = \delta$$

Algorithm I & II are applied for obtaining forward and backward differentials with probability 1. Then, we use miss-in-the-middle approach to construct 10 round impossible differential trail using algorithm III. We have used “||” symbol for concatenating 4 nibbles of 16-bit size.

Algorithm I: Forward Differential Trails:

1. First we start with assigning non-zero value α to any one branch X_i ($8 \leq i \leq 14$) and the values for the remaining branches X_j ($0 \leq j \leq 15$, $j \neq i$) must be set to zero. For i=13, we find one forward differential trail of 5 rounds in the following steps.
   Starting Difference: $0,0,0,0 \| 0,0,0,0 \| 0,0,0,0 \| 0,0,\alpha,0$
2. There is no application of S-box on the branch with value α, therefore we get the same output from Layer I and II. Application of Layer III leads to the following output from the first round with probability 1:
   Layer III: $0,0,0,0 \| 0,0,\alpha,0 \| 0,0,0,0 \| 0,0,0,0$
3. There is one application of S-box on α which outputs β in first Layer and application of all three layers return the following outputs from second round with probability 1:
   Layer I: $0,0,0,0 \| 0,0,\alpha,0 \| 0,\beta,0,0 \| 0,0,0,0$
   Layer II: $0,0,0,0 \| 0,0,\alpha,0 \| 0,\beta,0,0 \| 0,0,0,\alpha$
   Layer III: $0,\beta,0,0 \| 0,0,0,\alpha \| 0,0,0,0 \| 0,0,\alpha,0$
4. We have two nonzero values as input to S-box in this round, one application on α which outputs β and second application on β which outputs γ and we get the output from third round with probability 1 as follows applying all three layers:
   Layer I: $0,\beta,0,0 \| 0,0,0,\alpha \| \beta,0,0,0 \| 0,0,\alpha\oplus\gamma,0$
   Layer II: $0,\beta,0,0 \| 0,0,0,\alpha \| \beta,\alpha,\alpha,\alpha \| \alpha,\alpha,\gamma,\alpha\oplus\beta$
   Layer III: $\beta,\alpha,\alpha,\alpha \| \alpha,\alpha,\gamma,\alpha\oplus\beta \| 0,\beta,0,0 \| 0,0,0,\alpha$
5. There are four applications of S-box, one application on α which gives β, second application on β gives γ, third application on γ outputs δ and fourth application on $\alpha\oplus\beta$ output some undetermined value ?. The following outputs with probability 1 from three layers of fourth round are returned:
   Layer I: $\beta,\alpha,\alpha,\alpha \| \alpha,\alpha,\gamma,\alpha\oplus\beta \| ?,\beta\oplus\delta,\beta,\beta \| \beta, \beta,\beta,\alpha\oplus\gamma$
   Layer II: $\beta,\alpha,\alpha,\alpha \| \alpha,\alpha,\gamma,\alpha\oplus\beta \| ?,\alpha\oplus\delta,\alpha,\alpha \| \alpha,\alpha,\alpha,\alpha\oplus\beta$
   Layer III: $?,\alpha\oplus\delta,\alpha,\alpha \| \alpha,\alpha,\alpha,\alpha\oplus\beta \| \beta,\alpha,\alpha,\alpha \| \alpha,\alpha,\gamma,\alpha\oplus\beta$

6. There are four applications of S-box, one application on α gives β, second application on $\alpha\oplus\beta$ gives ?, third application on $\alpha\oplus\delta$ gives ? and fourth application on ? outputs some value ?. We get the following output in fifth round with probability 1:
   Layer I: $?,\alpha\oplus\delta,\alpha,\alpha \parallel \alpha,\alpha,\alpha,\alpha\oplus\beta \parallel ?,\alpha\oplus\beta,\alpha\oplus\beta,\alpha\oplus\beta \parallel \alpha\oplus\beta,\alpha\oplus\beta,?,?$
   Layer II: $?,\alpha\oplus\delta,\alpha,\alpha \parallel \alpha,\alpha,\alpha,\alpha\oplus\beta \parallel ?,0,0,0 \parallel 0,0,?,?$
   Layer III: $?,0,0,0 \parallel 0,0,?,? \parallel ?,\alpha\oplus\delta,\alpha,\alpha \parallel \alpha,\alpha,\alpha,\alpha\oplus\beta$

Algorithm II: Backward Differential Trails:

1. We assign value α to any one branch Y_i ($1 \le i \le 6$) and zero to other branches Y_j ($0 \le j \le 15$, $j\neq i$). For i=5, we find one backward differential trail of 5 rounds in the following steps.
   Ending Difference: $0,0,0,0 \parallel 0,\alpha,0,0 \parallel 0,0,0,0 \parallel 0,0,0,0$
2. There is no application of S-box on α due to EGFNs structure so there is no effect of Layer II and III on the input. Application of layer I returns the following output after one round with probability 1 in upward direction:
   Layer I: $0,0,0,0 \parallel 0,0,0,0 \parallel 0,0,0,0 \parallel 0,\alpha,0,0$
3. There is one application of S-box on α which gives β as output and we get the following probability 1 output of second round using all three layers:
   Layer III: $0,0,0,0 \parallel 0,\alpha,0,0 \parallel 0,0,0,0 \parallel 0,0,0,0$
   Layer II: $0,0,0,0 \parallel 0,\alpha,0,0 \parallel 0,0,0,0 \parallel 0,0,0,\alpha$
   Layer I: $0,0,0,0 \parallel 0,\alpha,0,0 \parallel 0,0,\beta,0 \parallel 0,0,0,\alpha$
4. There are two applications of S-box, one application on α which gives β and second application on β which gives γ as output and we get the following output of third round with probability 1 from all layers:
   Layer III: $0,0,\beta,0 \parallel 0,0,0,\alpha \parallel 0,0,0,0 \parallel 0,\alpha,0,0$
   Layer II: $0,0,\beta,0 \parallel 0,0,0,\alpha \parallel 0,\alpha,\alpha,\alpha \parallel \alpha,0,\alpha,\alpha\oplus\beta$
   Layer I: $0,0,\beta,0 \parallel 0,0,0,\alpha \parallel \beta,\alpha,\alpha,\alpha \parallel \alpha,\gamma,\alpha,\alpha\oplus\beta$
5. There are four applications of S-box, one application on α gives β, second application on β gives γ, third application on γ gives δ as output and fourth application on $\alpha\oplus\beta$ gives ?. The following outputs from fourth round with probability 1 is returned:
   Layer III: $\beta,\alpha,\alpha,\alpha \parallel \alpha,\gamma,\alpha,\alpha\oplus\beta \parallel 0,0,\beta,0 \parallel 0,0,0,\alpha$
   Layer II: $\beta,\alpha,\alpha,\alpha \parallel \alpha,\gamma,\alpha,\alpha\oplus\beta \parallel 0,\alpha\oplus\beta,\alpha,\alpha\oplus\beta \parallel \alpha\oplus\beta,\alpha\oplus\beta,\alpha\oplus\beta,\alpha\oplus\beta\oplus\gamma$
   Layer I: $\beta,\alpha,\alpha,\alpha \parallel \alpha,\gamma,\alpha,\alpha\oplus\beta \parallel ?,\alpha,\alpha\oplus\delta,\alpha \parallel \alpha,\alpha,\alpha,\alpha\oplus\beta$
6. There are four applications of S-box, one application on α gives β, second application on $\alpha\oplus\beta$ gives ?, third application on $\alpha\oplus\delta$ gives ? and fourth application on ? gives some value ? as output. We get the following outputs in fifth round with probability 1:
   Layer III: $?,\alpha,\alpha\oplus\delta,\alpha \parallel \alpha\ \alpha,\alpha,\alpha\oplus\beta \parallel \beta,\alpha,\alpha,\alpha \parallel \alpha,\gamma,\alpha,\alpha\oplus\beta$
   Layer II: $?,\alpha,\alpha\oplus\delta,\alpha \parallel \alpha,\alpha,\alpha,\alpha\oplus\beta \parallel \beta,\beta,\beta,\beta \parallel \beta,\alpha\oplus\beta\oplus\gamma,\beta,\delta$
   Layer I: $?,\alpha,\alpha\oplus\delta,\alpha \parallel \alpha,\alpha,\alpha,\alpha\oplus\beta \parallel ?,0,0,0 \parallel 0,?,0,?$

Algorithm III: Impossible Differential trail using miss-in-the-middle approach:

Finally we get the following 10 round impossible differential trail for any non-zero value α:

0, 0, 0, 0 ∥ 0, 0, 0, 0 ∥ 0, 0, 0, 0 ∥ 0, 0, α, 0
Probability 1↓ 5 FR
?, **0**, 0, **0** ∥ **0, 0**, ?, ? ∥ ?, ?, **α, α** ∥ **α**, α, **α**, ?
?, **α**, ?, **α** ∥ **α, α**, α, ? ∥ ?, 0, **0, 0** ∥ **0**, ?, **0**, ?
Probability 1↓5 BR
0, 0, 0, 0 ∥ 0, α, 0, 0 ∥ 0, 0, 0, 0 ∥ 0, 0, 0, 0

Table 2: 10 round Impossible Differential trail

We get several 10 round impossible differential trails by varying the positions for the non-zero difference α. We get these impossible differential trails either by showing a contradiction between two 5 round forward and backward differentials of probability 1 or by getting a contradiction between a 6 round forward differential and a 4 round backward differential each with probability 1. Some of the 10 round impossible differential trails are listed below:

S. No.	Start and End Differences (nonzero difference α)	No. of Rounds	Intermediate Differences (with contradictions α ≠ 0)
1	0,0,0,0∥0,0,0,0∥0,0,0,0∥0,α,0,0	5 FR→	?,0,0,0∥0,?,0,?∥?,α,?,α∥α,α,α,?
	0,0,0,0∥0,α,0,0∥0,0,0,0∥0,0,0,0	5 BR→	?,α,?,α∥α,α,α,?∥?,0,0,0∥0,?,0,?
2	0,0,0,0∥0,0,0,0∥0,0,0,0∥α,0,0,0	5 FR→	?,0,0,0∥?,0,0,?∥?,α,α,?∥α,α,α,?
	0,0,0,0∥α,0,0,0∥0,0,0,0∥0,0,0,0	5 BR→	?,α,α,?∥α,α,α,?∥?,0,0,0∥?,0,0,?
3	0,0,0,0∥0,0,0,0∥0,0,0,α∥0,0,0,0	5 FR→	?,0,0,?∥0,0,0,?∥?,α,α,α∥?,α,α,?
	0,0,0,α∥0,0,0,0∥0,0,0,0∥0,0,0,0	5 BR→	?,α,α,α∥?,α,α,?∥?,0,0,?∥0,0,0,?
4	0,0,0,0∥0,0,0,0∥0,0,α,0∥0,0,0,0	5 FR→	?,0,?,0∥0,0,0,?∥?,α,α,α∥α,?,α,?
	0,0,α,0∥0,0,0,0∥0,0,0,0∥0,0,0,0	5 BR→	?,α,α,α∥α,?,α,?∥?,0,?,0∥0,0,0,?
5	0,0,0,0∥0,0,0,0∥0,α,0,0∥0,0,0,0	5 FR→	?,?,0,0∥0,0,0,?∥?,α,α,α∥α,α,?,?
	0,α,0,0∥0,0,0,0∥0,0,0,0∥0,0,0,0	5 BR→	?,α,α,α∥α,α,?,?∥?,?,0,0∥0,0,0,?
6	0,0,0,0∥0,0,0,0∥0,0,0,0∥0,0,0,α	6 FR→	?,?,?,?∥?,?,?,?∥0,?,?,?∥?,?,?,?
	α,0,0,0∥0,0,0,0∥0,0,0,0∥0,0,0,0	4 BR→	?,β,β,β∥β,β,β,β∥γ,?,?,?∥?,?,?,?
7	0,0,0,0∥0,0,0,0∥α,0,0,0∥0,0,0,0	6 FR→	γ,?,?,?∥?,?,?,?∥?,β,β,β∥β,β,β,β
	0,0,0,0∥0,0,0,α∥0,0,0,0∥0,0,0,0	4 BR→	0,?,?,?∥?,?,?,?∥?,?,?,?∥?,?,?,?

Table 3: 10-round Impossible Differential trails

4. Impact of Analysis and further work

Security estimates of EGFNs for impossible differential attack were provided by authors in [1] and claim for the maximum number of rounds in the impossible differential were supported by $\mathcal{U}$-method. Our analysis indicates that $\mathcal{U}$-method does not give optimal results for this type of schemes and it should be analyzed for optimality to such schemes. The number of rounds in impossible differential trail may be increased further by relaxing the condition for input differentials. We can try with non-zero nibble values greater than one and the values should be taken in a way such that it cancels some of the intermediate values.

5. Conclusion:

An Encryption scheme with less number of rounds in impossible differentials is considered more secure and greater the number of rounds in impossible differentials gives an attack on more rounds of the scheme. We have added one round in impossible differential of EGFNs scheme to the claim of authors. We have provided several 10 round differential trails for this scheme which can be easily applied to new block cipher proposals based on EGFNs scheme. We have increased the number of rounds in impossible differential claimed by authors for all block sizes which also indicates that $\mathcal{U}$-method does not give correct estimates of security for EGFNs.

Acknowledgements: First author is thankful to Dr G Athithan, Director SAG and Ms Pratibha Yadav for their valuable guidance and continuous support. He would also like to thank Dr Dhananjoy Dey and Mr. Bhartendu Nandan for their valuable comments and suggestions.

References:

1. Berger, T.P.; Minier, M. and Thomas, G, “Extended Generalized Feistel Networks using Matrix Representation”. In SAC 2013, Vol. 8282, LNCS, pp. 289-305, Springer, 2013
2. Biham, E. and Shamir, A., “Differential cryptanalysis of DES-like cryptosystems”. In Advances in Cryptology CRYPTO 1990, Vol. 537, LNCS, pp. 2-21, Springer, 1990
3. Biham, E.; Biryukov, A. and Shamir, A., “Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials”. In Advances in Cryptology EUROCRYPT 1999, Vol. 1592, LNCS, pp. 12-23, Springer, 1999
4. Bogdanov, A. and Shibutani., K, “Generalized Feistel networks revisited”, Designs, Codes and Cryptography, Vol. 66, Issue 1-3, pp. 75-97, Springer 2013
5. Daemen, J. and Rijmen, V., “The Design of Rijndael”, Berlin: Springer-Verlag, 2002
6. Hoang, V.T. and Rogaway, P., “On Generalized Feistel Networks”. In Advances in Cryptology CRYPTO 2010, Vol. 6223, LNCS, pp. 613-630, Springer, 2010
7. Kim, J.; Hong, S. and Lim, J., “Impossible differential cryptanalysis using matrix method”. Discrete Mathematics, Vol. 310(5), pp. 988-1002, 2010
8. Kumar, M.; Pal, SK and Panigrahi, A., “Some Results on Design Parameters of Lightweight Block Ciphers” In Bilingual International Conference on Information Technology: Yesterday, Today, and Tomorrow, pp. 81-85, DESIDOC, 2015
9. Luo, Y.; Wu, Z.; Lai, X. and Gong, G., “A Unified Method for Finding Impossible Differentials of Block Cipher Structures”. IACR Cryptology e-Print Archive, 627, 2009
10. National Bureau of Standards, U. S., “Data Encryption Standard”, 1977
11. Nyberg, K., “Generalized Feistel Networks”. In Advances in Cryptology ASIACRYPT 1996, Vol. 1163, LNCS, pp. 91-104, Springer, 1996
12. Schneier, B. and Kelsey, J., “Unbalanced Feistel Networks and Block-Cipher Design”, In FSE 1996, LNCS, pp. 121-144, 1996
13. Sorkin, A., “LUCIFER: a cryptographic algorithm”, *Cryptologia*, Vol. **8**(1), pp. 22–35, 1984
14. Suzaki, T. and Minematsu, K., “Improving the generalized Feistel”. In FSE 2010, Vol. 6147, LNCS, pp. 19-39, Springer, 2010
15. Yanagihara, S. and Iwata, T., “Improving the Permutation Layer of Type 1, Type 3, Source-Heavy, and Target-Heavy Generalized Feistel Structures” IEICE Trans, Vol. 96-A(1), pp. 2-14, 2013
16. Zhang, L. and Wu, W., “Differential Cryptanalysis of Extended Generalized Feistel Networks” , Information Processing Letters, Vol. 114, Issue 12, pp. 723-727, Elsevier, 2014