Information Processing Letters 114 (2014) 723–727

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Differential analysis of the Extended Generalized Feistel Networks ☆

Lei Zhang [a,*], Wenling Wu [a,b]

[a] TCA, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
[b] State Key Laboratory of Computer Science, Institute of Software, Beijing 100190, China

ARTICLE INFO

Article history:
Received 25 January 2014
Received in revised form 17 June 2014
Accepted 4 July 2014
Available online 11 July 2014
Communicated by V. Rijmen

Keywords:
Cryptography
Block cipher
EGFN
Active S-box number
Iterative differential

ABSTRACT

This paper studies the differential analysis of Extended Generalized Feistel Networks (EGFNs). First we construct a class of differential characteristics which conflict with designers' evaluation of minimal number of active S-boxes for EGFN. Then by analyzing the difference cancellation property of EGFN, we propose a method to search a special type of differential characteristics with high probability. We obtain the best case of this kind of differential characteristic for EGFN with block number $4 \le k \le 32$. Our results show that for EGFN with $k \ge 8$ there always exist high probability iterative differential characteristics and their number of active S-boxes for 20-round all are equal to 26. Therefore, the actual ability of EGFN resisting differential analysis may be a lot weaker than evaluated by designers and larger block size cannot improve the situation.

1. Introduction

Recently, researches on the design of Generalized Feistel Networks (GFNs) have received lots of attention and many new ideas have been proposed. Among them, some novel and well designed structures were proposed, and they led to some interesting researches which improved previous results greatly. Roughly speaking, there are many variants of GFNs, such as Source-Heavy as in RC2 [5], Target-Heavy as in MARS [3], Type-1 as in CAST-256 [1], Type-2 as in CLEFIA [6], Type-3 and Nyberg's GFNs [4], etc. Usually, GFNs perform a cyclic shift of sub-blocks at the end of each round. Then in 2010, Suzaki et al. proposed a kind of improved generalized Feistel structure in [7] and its variant was already applied in the design of TWINE [8]. Its main idea was to replace the cyclic shift of sub-blocks in Type-2 GFN with an even–odd sub-block permutation, which could improve the diffusion property and security against classical attacks efficiently. Then Yanagihara and Iwata [9] further studied the case of Type-1, Type-3, Source-Heavy and Target-Heavy GFNs with non-cyclic permutation. They analyzed the maximum diffusion round and security evaluations, respectively.

Moreover, in SAC 2013 Berger et al. [2] presented a unified vision of GFNs using a matrix representation and used it to further study the diffusion properties of GFNs. They also extended this matrix representation and proposed a broader class of Feistel networks called Extended Generalized Feistel Networks (EGFNs). Here in addition to non-cyclic permutation they also applied XOR operations between sub-blocks to enhance the diffusion effect. Finally, they proposed one particular construction of EGFN with good diffusion properties and evaluated the security of this kind of EGFN under two instantiation examples against classical attacks and security models.

However, in this paper we find that there are some mistakes in their security evaluation of EGFN against

☆ This work was partially supported by the National Natural Science Foundation of China (Nos. 61202420, 61272476, 61232009) and the National Basic Research Program of China (No. 2013CB338002).

* Corresponding author.
E-mail addresses: zhanglei@tca.iscas.ac.cn (L. Zhang), wwl@tca.iscas.ac.cn (W. Wu).

http://dx.doi.org/10.1016/j.ipl.2014.07.001
0020-0190/

differential cryptanalysis. We can construct a class of differential characteristics which conflict with their evaluation of minimal number of active S-boxes for EGFN. Then by analyzing the difference cancellation property of EGFN, we propose a method to search a special type of differential characteristics with high probability. We obtain the best cases of this kind of differential characteristic for EGFN with $4 \le k \le 32$, and analyze the pattern and count of this kind of characteristic in detail. Our results show that for EGFN with $k \ge 8$ there always exist high probability iterative differential characteristics and their number of active S-boxes for 20-round all are equal to 26. Therefore, although EGFNs have good diffusion property, their ability to resist against differential analysis may be a lot weaker than evaluated and larger block size cannot improve the situation. Especially, for the widely used cases of $k = 8, 16, 32$, we analyze the application of EGFN in cipher design and study the choice of non-linear S-box and especially the number of rounds briefly.

The rest of the paper is organized as follows. Section 2 describes the construction of EGFNs and their security evaluations. Section 3 presents our example of a class of differential characteristics which conflict with designers' security evaluation of EGFN. Section 4 analyzes difference cancellation property of EGFN, and proposes a method to search maximum probability differential characteristic under a special condition. Section 5 analyzes the search results and studies application of EGFNs in cipher design briefly. Section 6 concludes the paper.

2. Extended Generalized Feistel Networks

In SAC 2013, Berger et al. [2] proposed a new kind of Feistel-type networks called Extended Generalized Feistel Networks (EGFNs). Their main idea was to use a linear mapping instead of block-wise permutation to further improve the diffusion effect. Moreover, in order to reserve the quasi-involutive property and reduce the implementation cost, they proposed a three-layer structure. The first layer was a traditional GFN round function layer with non-linear functions F. The second layer was also a GFN but with the identity mapping as round-functions, namely in the matrix representation with I off-diagonal non-zero coefficients instead of F. Finally, the last layer P was a permutation matrix. Therefore, the combination of non-linear round-functions F and identity round-functions I provided cryptographic security and quick diffusion respectively. They called these new schemes Extended Generalized Feistel Networks (EGFNs), and for formal definition one could refer to [2] for more information.

As an efficient example of EGFN, they proposed a particular construction with good full diffusion delay and cheap cost. This EGFN consists of k sub-blocks and $s = k/2$ round-functions F, and its matrix representation $M_{k\times k}$ can be depicted as follows. Here the parameter F (I) is a formal parameter, meaning it merely indicates the presence of a round-function (identity-function) and the same F is used for all different round-functions throughout the cipher. Then for indices $0 \le i, j \le k-1$, coefficient at row i and column j of matrix $M_{k\times k}$ is either 1 if y_i directly depends on x_j, or a formal parameter F (I) if y_i depends on x_j via a round-function (identity-function), or 0 otherwise.

$$M_{k\times k} = \begin{pmatrix} & & & & F & 1 & & & & \\ & (0) & & F & I & & 1 & & & \\ & & \iddots & & I & & & \ddots & & \\ & F & & (0) & \vdots & & & & 1 & \\ F & I & I & \cdots & I & & & & & 1 \\ 1 & & & & & & & & & \\ & 1 & & & & & & & & \\ & & \ddots & & & & & (0) & & \\ & & & 1 & & & & & & \\ & & & & 1 & & & & & \end{pmatrix}$$

They also analyzed the diffusion property and security evaluation of this special construction of EGFN. For an even integer $k \ge 4$, the k-block EGFN defined above can achieve full diffusion in $d = 4$ rounds. Compared with the family of improved GFNs proposed in [7] which diffused in $d = 2\log_2^k$ rounds, EGFN could achieve full diffusion faster and also at a cheaper cost. They also analyzed the proposed EGFN with essentially $k = 8$ and $k = 16$ as instantiate examples regarding the pseudorandomness and resistance to classical attacks. Especially, in the evaluation of security against differential/linear cryptanalysis, they claimed that there are at least 39 and 74 active S-boxes in 20 rounds for $k = 8$ and $k = 16$ respectively, which was much better than the results of [7]. Table 1 lists the comparison of minimal number of active S-sboxes evaluation up to 20 rounds for EGFN [2] and improved GFN [7].

3. Differential characteristic for EGFN with $k = 8$

Here we take EGFN with $k = 8$ as example, and study its security against differential attack. We construct a special class of differential characteristics which conflict with the evaluation of minimal number of active S-boxes in [2].

Considering the construction of EGFN with $k = 8$, there are only four non-linear functions F together with several XOR operations in each round. Usually, F can be considered as a classical n-bit S-box construction. Namely, we can write the internal n-bit function F as $F(x) = S(K \oplus x)$ where K is a subkey different at each round. Similar assumption was used in the security evaluation in [2], and F with non-zero input difference $\alpha \ne 0$ corresponded to the active S-box. Then for any possible differential probability $DP_F(\alpha \to \alpha) \ne 0$ with respect to the differential distribution table of the S-box F, we can construct a special class of 3-round iterative differential characteristics for EGFN with $k = 8$ as follows. The differential propagation is also illustrated in Fig. 1.

$$(0,0,0,0,\ 0,\alpha,\alpha,0) \xrightarrow{3R} (0,0,0,0,\ 0,\alpha,\alpha,0)$$