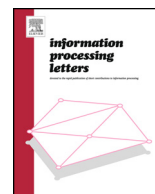




ELSEVIER

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 $4 \leq k \leq 32$. Our results show that for EGFN with $k \geq 8$ 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.

© 2014 Elsevier B.V. All rights reserved.

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, Suzuki 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).

Download English Version:

<https://daneshyari.com/en/article/427332>

Download Persian Version:

<https://daneshyari.com/article/427332>

[Daneshyari.com](https://daneshyari.com)