Information Processing Letters 112 (2012) 427–432

Contents lists available at SciVerse ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

The provable constructive effect of diffusion switching mechanism in CLEFIA-type block ciphers

Qingju Wang [a,b], Andrey Bogdanov [b,*]

[a] Shanghai Jiao Tong University, Department of Computer Science and Engineering, Shanghai, China
[b] Katholieke Universiteit Leuven, ESAT/COSIC and IBBT, Leuven, Belgium

ARTICLE INFO

Article history:
Received 14 December 2011
Received in revised form 13 February 2012
Accepted 13 February 2012
Available online 15 February 2012
Communicated by D. Pointcheval

Keywords:
Cryptography
Block ciphers
Generalized Feistel networks
CLEFIA
Diffusion switching mechanism
Substitution diffusion networks
Linear cryptanalysis
Efficiency

ABSTRACT

CLEFIA is a block cipher designed by Sony Corporation, adopted as a lightweight encryption algorithm of the new ISO/IEC 29192-2 standard, and proposed as a Japanese e-Government recommendation cipher CRYPTREC candidate.
Provable security properties of cryptographic design are crucial in any security evaluation. Providing lower bounds on the number of active S-boxes in differential and linear characteristics has been one of the few important provable properties that can be formally shown for block ciphers and hence received a lot of attention.
In this work, we prove tighter lower bounds on the number of linearly active S-boxes in CLEFIA-type generalized Feistel networks (GFNs) with diffusion switching mechanism (DSM). We show that every 6 rounds of such GFNs provide 50% more linearly active S-boxes than proven previously. Moreover, we experimentally demonstrate that the new bound is tight for up to at least 12 rounds, whereas the previous one is not. Thus, this paper delivers first *provable* evidence that diffusion switching mechanism actually provides an advantage by guaranteeing more active S-boxes in GFNs.

1. Introduction

1.1. Motivation

Generalized Feistel networks (GFNs) [18] have been popular with the designers of symmetric-key cryptographic primitives including block ciphers, stream ciphers and hash functions. They offer a simple way of domain extension given a function with good cryptographic properties. Probably the best understood structure of its round transform relies on substitution–diffusion functions (SD-functions) — a brick layer of local nonlinear permutations (*S-boxes*) followed by a multiplication by a *diffusion matrix* over a binary finite field (*linear diffusion*).

GFN_4 are 4-line generalized Feistel networks. Type-I and type-II GFN_4 are referred to as GFN_4-I and GFN_4-II, respectively, throughout this paper (Figs. 1 and 2). The findings of [5] indicate that going from single SD-functions [19, 11] to double SD-functions improves the efficiency of GFN_4 by up to 33% for GFN_4-I and by up to 50% for GFN_4-II, as measured by the proportion of differentially and linearly S-boxes in all S-boxes of the cipher. The work [5] proves that for GFN_4 with double SD-functions every 14 rounds of GFN_4-I and every 6 rounds of GFN_4-II add $7\mathcal{B}$ and $6\mathcal{B}$ differentially and linearly active S-boxes, respectively, where $\mathcal{B}$ is the branch number of the diffusion matrix M (or its transpose) used in the round functions. Underlying SD-type functions can differ depending on:

- **Number of distinct diffusion matrices:** The standard approach is to use a single matrix in all rounds and functions (*single-round diffusion*), e.g. applied in Camellia [1]. The alternative approach proposed in [13] is to employ two and more distinct diffusion matrices in different rounds and functions (*multiple-round diffusion*, or *diffusion switching mechanism, DSM*), which

* Corresponding author.
E-mail addresses: qingju.wang@esat.kuleuven.be (Q. Wang), andrey.bogdanov@esat.kuleuven.be (A. Bogdanov).

0020-0190/$ – see front matter
doi:10.1016/j.ipl.2012.02.006

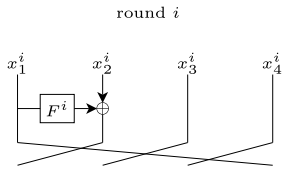

Fig. 1. GFN$_4$-I.

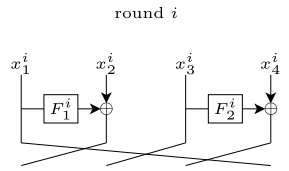

Fig. 2. CLEFIA-type GFN$_4$-II.

prevents difference and linear mask cancelation at XORs, e.g. utilized in CLEFIA [14].

- **Number of SD-layers in a function:** SD-type functions usually consist of a single SD-layer (*single SD-functions*), as e.g. those in CLEFIA [14] and Camellia [1]. In some ciphers, however, SD-type functions have double SD-layers (*double SD-functions*), e.g. in E2 [8] and Piccolo [12].

CLEFIA is a recent block cipher designed by Sony Corporation, adopted as a lightweight encryption algorithm of the new ISO/IEC 29192-2 standard, and proposed as a CRYPTREC Japanese e-Government recommendation cipher. The design of CLEFIA is a 4-line type-II GFN (*GFN$_4$-II*) with DSM and single SD-functions. GFN$_4$-II belongs to the type of GFNs. The structure that we will be investigating in this paper is the d-line type-II GFN with DSM and single SD-functions, GFN$_d$-II.

1.2. Previous work on GFN$_d$-II

GFN$_d$-II with other types of SD-type functions have been thoroughly studied in the literature, see Table 1.

Tight lower bounds on the number of both differentially and linearly active S-boxes for GFN$_4$-II with single SD-functions and single-round diffusion are obtained in [11]: Every 6 rounds of GFN$_4$-II are proven to provide at least $2\mathcal{B}$ active S-boxes, where $\mathcal{B}$ is the differential and linear branch number of the diffusion matrices used in the round functions.

Tight minimum numbers of differentially and linearly active S-boxes for GFN$_4$-II with double SD-functions and single-round diffusion are proven in [5]. The findings of [5] indicate that going from single SD-functions [11] to double SD-functions improves the efficiency of GFN$_4$-II by up to 50%, as measured by the proportion of differentially and linearly S-boxes in all S-boxes of the cipher. The work [5] proves that every 6 rounds of GFN$_4$-II with double SD-functions add at least $6\mathcal{B}$ active S-boxes for both differential and linear cryptanalysis.

Bounds on the number of differentially and linearly active S-boxes for GFN$_4$-II with single SD-functions and DSM were obtained in [15]. It is proven that every 6 rounds add at least $2\mathcal{B}$ differentially and linearly active S-boxes. However, this bound is not tight, especially for the number of linearly active S-boxes. In fact, the bound proven in [15] for DSM yields a lower number of differentially and linearly active S-boxes than for single-round diffusion. So there has been no proof so far that DSM has any advantage over single-round diffusion. This paper will improve upon this.

1.3. Contributions of this paper

In this work, we prove that every 6 rounds of GFN$_d$-II with multiple-round diffusion (diffusion switching mechanism) and single SD-functions add at least $3\mathcal{B}$ linearly active S-boxes, see Table 1. This is exactly the construction behind the design of the lightweight block cipher CLEFIA, for the case of $d = 4$. $\mathcal{B}$ is the branch number of the single- and multiple-round diffusion matrices (their transposed inverses) used in the round functions. We experimentally demonstrate that the new bound is tight for up to at least 12 rounds, whereas the previous one is not.

The relevance of this bound is three-fold:

- This result indicates that the efficiency of CLEFIA-type GFNs is 50% higher than previously proven, in terms of the proportion of linearly active S-boxes in all S-boxes. This efficiency metric E is a valid efficiency metric introduced in [16] and used in [2–5]. Its definition can be found in Definition 1.
- Moreover, the new result suggests that the efficiency of GFN$_d$ with SD-type functions is equally improved both by moving from single to double SD-functions [5] and by going from single-round diffusion to DSM over multiple rounds — the central contribution of this paper.
- Our bounds constitute also the first provable evidence that GFNs with DSM can actually provide more active S-boxes than GFNs with single-round diffusion. Previously [14,15], for GFNs, this advantage has been only demonstrated experimentally for some concrete CLEFIA-like examples.

2. Preliminaries

2.1. GFN$_4$ with SD-functions

Type-I and type-II GFNs are block ciphers with the state equally divided into an even number $d \geqslant 4$ lines. They are referred to as GFN$_d$-I and GFN$_d$-II in this paper. The structures of GFN$_d$-I and GFN$_d$-II when $d = 4$ are as shown in Figs. 1 and 2. In one round of both GFN$_4$-I and GFN$_4$-II, let the input x^i of round i be $x^i = (x_1^i, x_2^i, x_3^i, x_4^i)$. Then the output of GFN$_4$-I and for GFN$_4$-II will be $(x_2^i \oplus F^i(x_1^i), x_3^i, x_4^i, x_1^i)$ and $(x_2^i \oplus F_1^i(x_1^i), x_3^i, x_4^i \oplus F_2^i(x_3^i), x_1^i)$ respectively, for some keyed nonlinear functions F^i, F_1^i and F_2^i. F_j^i often exhibits the substitution–diffusion (SD) structure. Here, the subkey addition followed by a layer of m S-boxes, $s_i, i = 1, \ldots, m$, and an $m \times m$ linear diffusion mapping M_j^i over a binary finite field. Such F-functions are called *SD-functions*. The structure of SD-functions is depicted in Fig. 3.