Provable Security for a 4-blocked Unbalanced Feistel Structure Against Differential Cryptanalysis

Hamid Mala[1], Mohammad Dakhilalian[2], Mahdi Sajadieh[3]

Electrical & Computer Engineering Department,
Isfahan University of Technology, Isfahan, Iran
[1]hamid_mala@ec.iut.ac.ir, [2]mdalian@ec.iut.ac.ir, [3]sadjadieh@ec.iut.ac.ir

Abstract

In this paper, we show that the 4-blocked unbalanced Feistel structure is provably secure against differential cryptanalysis. The main result of this paper is that the 13-round differential probability of this structure is upperbounded by $p^2+ p^3+ p^5$ if the maximum differential probability of a round function is p

Keywords

Provable security, block cipher, differential cryptanalysis, unbalanced Feistel structure

1. Introduction

The most well known method of analizing block ciphers is Differential Cryptanalysis(DC) which was invented by Biham and Shamir in 1990 [1]. The general purpose of a differential attack is to find the first or the last round keys with a complexity less than an exhaustive search for a master key by using a differential characteristic with a high probability. However the maximum characteristic probability may not guarantee a block cipher to be secure against DC even if it is sufficiently small. In order to show that a block cipher is secure against DC, we should prove the maximum differential probability is upperbounded by a small enough value. Roughly speaking a "differential" is a collection of "characteristic"s. Therefore a block cipher is called to have *provable security* against DC, if the upper bounds of the maximum of differential probabilities is sufficiently small, and a block cipher is called to have *practical security*, if the upper bounds of the maximum of differential characteristics is sufficiently small.

The other powerful attack on block ciphers is Linear Cryptanalysis (LC) which was invented by Matsui[2]. Similarly we can define practical security and provable security against LC. However the main purpose of this paper is the provable security against DC, and we will not consider provable security against LC.

Nyberg and Knudsen first proposed the concept of provable security against DC and gave a provable security for a Feistel structure in 1992[3]. In [4] Nyberg also proposed a conjecture that if a Generalized Feistel Network(GFN) has n parallel bijective F functions per round then the average probability of each differential over at least $3n$ rounds is upperbounded by p^{2n}, where p is the maximum average probability of the F function. In [4] Matsui introduced the block cipher MISTY with provable security against DC and LC. Furthermore, Sung et al. and Hong et al. showed a provable security for a SKIPJACK-like and a SPN structure respectively[5,6,7]. Recently Lee et al. showed a provable security for a RC6-like structure and a MISTY-FO-like structure against DC[8]

Since AES has been proposed, the 128-bit block ciphers are usually adopted. If we construct 128-bit block ciphers with the Feistel structure, we need to design 64-bit round function. However, to design a 64-bit round function is usually more difficult than to design a 32-bit one. So the unbalanced Feistel networks (UFN) were proposed and used in CAST-256, MARS, RC6, TWOFISH, etc. Figure 1 shows