Recursive Diffusion Layers for Block Ciphers and Hash Functions

Mahdi Sajadieh[1], Mohammad Dakhilalian[1], Hamid Mala[2], and Pouyan Sepehrdad[3,⋆]

[1] Cryptography & System Security Research Laboratory, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran
sadjadieh@ec.iut.ac.ir, mdalian@cc.iut.ac.ir
[2] Department of Information Technology Engineering, University of Isfahan, Isfahan, Iran
h.mala@eng.ui.ac.ir
[3] EPFL, Lausanne, Switzerland
pouyan.sepehrdad@epfl.ch

Abstract. Many modern block ciphers use maximum distance separable (MDS) matrices as the main part of their diffusion layers. In this paper, we propose a new class of diffusion layers constructed from several rounds of Feistel-like structures whose round functions are linear. We investigate the requirements of the underlying linear functions to achieve the maximal branch number for the proposed 4×4 words diffusion layer. The proposed diffusion layers only require word-level XORs, rotations, and they have simple inverses. They can be replaced in the diffusion layer of the block ciphers MMB and Hierocrypt to increase their security and performance, respectively. Finally, we try to extend our results for up to 8×8 words diffusion layers.

Keywords: Block ciphers, Diffusion layer, Branch number, Provable security.

1 Introduction

Block ciphers are one of the most important building blocks in many security protocols. Modern block ciphers are cascades of several rounds and each round consists of confusion and diffusion layers. In many block ciphers, non-linear substitution boxes (S-boxes) form the confusion layer, and a linear transformation provides the required diffusion. The diffusion layer plays an efficacious role in providing resistance against the most well-known attacks on block ciphers, such as differential cryptanalysis (DC) [2] and linear cryptanalysis (LC) [10].

In 1994, Vaudenay [15,16] suggested using MDS matrices in cryptographic primitives to produce what he called multipermutations, not-necessarily linear

⋆ This work has been supported in part by the European Commission through the ICT program under contract ICT-2007-216646 ECRYPT II.

A. Canteaut (Ed.): FSE 2012, LNCS 7549, pp. 385–401, 2012.