www.ietdl.org

Published in IET Information Security
Received on 5th September 2009
Revised on 2nd September 2011
doi: 10.1049/iet-ifs.2010.0289

ISSN 1751-8709

Perfect involutory diffusion layers based on invertibility of some linear functions

M. Sajadieh[1] *M. Dakhilalian*[1] *H. Mala*[2]

[1]*Cryptography System Security Research Laboratory, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran*
[2]*Department of Information Technology Engineering, University of Isfahan, Isfahan, Iran*
E-mail: sadjadieh@ec.iut.ac.ir

Abstract: One of the most important structures used in modern block ciphers is the substitution–permutation network (SPN) structure. Many block ciphers with this structure widely use Maximun Distance Separable (MDS) matrices over finite fields as their diffusion layers, for example, advanced encryption standard (AES) uses a 4 × 4 MDS matrix as the main part of its diffusion layer and the block cipher Khazad has an involutory 8 × 8 matrix. In this study, first a construction is proposed for a 4 × 4 linear diffusion layer that can intermix four words of arbitrary size with branch number 5. Then extend this idea for 8 × 8 diffusion layer using low-cost linear functions. In this construction, first, certain binary linear combinations of inputs are fed into two or three different invertible linear functions and then combined using XOR operation. In order to show the efficiency of the proposed diffusion layer, the authors exploit it in a nested SPN structure and compare its efficiency with some well-known diffusion layers such as the diffusion layer of Hierocrypt.

Nomenclature

$\oplus$	the bit-wise XOR operation
&	the bit-wise AND operation
L_i, $i = 1, 2, 3$	any linear function
$(L_1 \oplus L_2)(x)$	$L_1(x) \oplus L_2(x)$
$L_1L_2(x)$	$L_1(L_2(x))$
$L_1^2(x)$	$L_1(L_1(x))$
$x \gg m(x \ll m)$	shift of a bit string x by m bits to the right (left)
$x \ggg m(x \lll m)$	circular shift of a bit string x by m bits to the right (left)
$\lvert\cdot\rvert$	determinant of a matrix in GF(2)
$I(\cdot)$ function	identity function ($I(x) = x$)
$a\|b$	the concatenation of two bit strings a and b
$x_{(n)}$	an n-bit value x
S_n	an n-bit S-box

1 Introduction

Modern block ciphers are cascades of confusion and diffusion layers. The confusion layer is made up of small non-linear substitution boxes (S-boxes). The goal of the diffusion (permutation) layer, which is often a linear transformation, is to diffuse the output of these small S-boxes. The diffusion layer plays an effective role in providing resistance against the most well-known attacks on block ciphers, differential cryptanalysis (DC) [1] and linear cryptanalysis (LC) [2].

The strength of a diffusion layer is usually quantified by the notion of branch number. A block cipher whose diffusion layer has a small branch number, may have critical weaknesses against DC and LC, even though its substitution layer consists of strong S-boxes. Many block ciphers, for example, AES, Anubis and Khazad use linear perfect diffusion primitives, that is, Maximun Distance Separable (MDS) matrices, in their diffusion layers [3–7]. Owing to the small size of their inputs (usually 8-bit words), MDS matrices are usually implemented by lookup-tables. MDS matrices with big sizes for their inputs/outputs are rarely exploited in block ciphers. As an exception, the block cipher Hierocrypt uses a diffusion layer that may be considered as an MDS matrix with four 32-bit input words [8, 9]. This diffusion layer reduces the efficiency of Hierocrypt in the software implementation.

In [10], a 16 × 16 MDS matrix has been proposed as a perfect diffusion layer for 128-bit block ciphers, but the size of the corresponding lookup-tables and the number of the required XOR operations are too large to be efficiently implemented neither in hardware nor in software. Thus, increasing the size of MDS matrix or the length of its inputs/outputs will decrease its efficiency.

The design of involutory diffusion transformations is an interesting direction in the designing of block ciphers. These transformations have the advantage that both the encryption and decryption processes are similar. Thus, they