Linear Cryptanalysis of DES Cipher (I)

(Version 1.03)

Mitsuru Matsui

Computer & Information Systems Laboratory
Mitsubishi Electric Corporation
5-1-1, Ofuna, Kamakura, Kanagawa, 247, Japan
matsui@mmt.isl.melco.co.jp

Abstract

This paper introduces a new methodology for cryptanalysis of block ciphers. The principle is based on a new measure of linearity and effectively applicable to Data Encryption Standard (DES). We give an explicit description of the best linear approximate expression and its approximate probability for DES and develop our analysis into the first successful known-plaintext attack faster than an exhaustive key search. As a result, DES is breakable with 2^{45} random known-plaintexts and the corresponding ciphertexts. Moreover, this method enables us to take the initial step toward a ciphertexts-only attack of block ciphers.

Key words: Data Encryption Standard, Block Cipher, Linear Cryptanalysis, Known-plaintext Attack.

1 Introduction

Data Encryption Standard (DES) [6], the first digital cipher whose structure was made public officially, is widely used as an international standard of cryptosystems for civilian applications, and generally accepted as an excellent model of a block cipher. At the same time, discussions on security of DES have been also active since the first appearance. The adequacy of the 56-bit key length, for example, has been the subject of controversy, and the secrecy of design criteria of S-boxes has provoked a great deal of public interest. Cryptanalysis of DES, especially study of S-boxes, has been a main research topic on block ciphers accordingly.

One of successful approaches to analysis of S-boxes is an observation of how changing input bits affects output bits. The first paper of cryptanalysis of DES [4] reported many remarkable characteristics of S-boxes including the fact that changing one input bit results in changing at least two output bits. Desmedt, Quisquater and Davio [3] generalized these criteria to obtain several new properties about relationship between various input changes and the corresponding output changes. To extend these local properties of S-boxes to the entire cipher structure, however, one had to wait for Differential Cryptanalysis by Biham and Shamir [1].