Block Cipher Analysis

Block ciphers are cryptographic primitives that operate on fixed size texts (blocks). Most designs aim towards secure and fast encryption of large amounts of data. Block ciphers also serve as the building block of a number of hash functions and message authentication codes (MAC). The task of cryptanalysis is to ensure that no attack violates the security bounds specified by a generic attack namely exhaustive key search and table lookup attacks. This thesis contains a general introduction to cryptography with focus on block ciphers and important block cipher designs, in particular the Advanced Encryption Standard (AES). We describe the most general types of block cipher cryptanalysis but concentrate on the algebraic attacks. While the algebraic techniques have been successful on certain stream ciphers, their application to block ciphers has not shown any significant results so far. This thesis contributes to the field of algebraic attacks on block ciphers by an analytic and systematic approach that allows insight to the techniques. Moreover, a new procedure of generating and applying probabilistic equations in algebraic attacks on block cipher is proposed and examined. Also, we present practical results, which to our knowledge are the best algebraic results on small scale variants of AES. In the final part of the thesis we present a new block cipher proposal Present and examine its security against algebraic and differential cryptanalysis in particular.

General information
Publication status: Published
Organisations: Discrete mathematics, Department of Mathematics
Contributors: Miolane, C. V.
Number of pages: 176
Publication date: Mar 2009

Publication information
Place of publication: Kgs. Lyngby, Denmark
Publisher: Technical University of Denmark (DTU)
Original language: English
Keywords: AES, differential, block, cipher, attack, Present Noekeon, algebraic
Electronic versions:
thesis_cvm_v1.pdf
Source: orbit
Source-ID: 240768