The Rabbit Stream Cipher - Design and Security Analysis

The stream cipher Rabbit was first presented at FSE 2003 [6]. In the paper at hand, a full security analysis of Rabbit is given, focusing on algebraic attacks, approximations and differential analysis. We determine the algebraic normal form of the main nonlinear parts of the cipher as part of a comprehensive algebraic analysis. In addition, both linear and nonlinear approximations of the next-state function are presented, as well as a differential analysis of the IV-setup function. None of the investigations have revealed any exploitable weaknesses. Rabbit is characterized by high performance in software with a measured encryption/decryption speed of 3.7 clock cycles per byte on a Pentium III processor.

General information
State: Published
Organisations: Cryptico A/S
Contributors: Boesgaard, M., Pedersen, T., Petersen, M. V., Zenner, E.
Pages: 7-29
Publication date: 2004

Host publication information
Title of host publication: Workshop Record SASC 2004
Place of publication: Online
Publisher: http://www.ecrypt.eu.org/stvl/sasc/record.html
Source: orbit
Source-ID: 197404
Research output: Research - peer-review › Article in proceedings – Annual report year: 2004