Cryptanalysis of Some Lightweight Symmetric Ciphers - DTU Orbit (13/12/2018)

Cryptanalysis of Some Lightweight Symmetric Ciphers

In recent years, the need for lightweight encryption systems has been increasing as many applications use RFID and sensor networks which have a very low computational power and thus incapable of performing standard cryptographic operations. In response to this problem, the cryptographic community designed a number of lightweight cryptographic primitives that varies from stream ciphers, block ciphers and recently to hash functions.

Out of these many lightweight primitives, the block cipher PRESENT gets a lot of attention from the cryptographic community and it has been recently adopted by ISO as one of the international standards in lightweight cryptography. This thesis aims at analyzing and evaluating the security of some the recently proposed lightweight symmetric ciphers with a focus on PRESENT-like ciphers, namely, the block cipher PRESENT and the block cipher PRINTcipher.

We provide an approach to estimate the probability of differential and linear approximations with low-weight differential and linear characteristics on PRESENT-like ciphers as well as ciphers allowing low hamming weight differential and linear characteristics. We study the effect of key scheduling in the distribution of linear approximations on a variant of PRESENT with identical round keys. We propose a new attack named the Invariant Subspace Attack that was specifically mounted against the lightweight block cipher PRINTcipher. Furthermore, we mount several attacks on a recently proposed stream cipher called A2U2.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology
Contributors: Abdelraheem, M. A. A. M. A., Knudsen, L. R., Zenner, E., Leander, G.
Number of pages: 123
Publication date: 2012

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Electronic versions:
orbit_thesis.pdf
Research output: Research › Ph.D. thesis – Annual report year: 2013