Secure Block Ciphers - Cryptanalysis and Design - DTU Orbit (31/12/2018)

Secure Block Ciphers - Cryptanalysis and Design

The rapid evolution of computational devices and the widespread adoption of digital communication have deeply transformed the way we conduct both business and everyday life and they continue to do so. The ability to ensure confidentiality and integrity of information sent over digital channels is fundamental to this development and is absolutely essential for all private and corporate communication, ranging from bank transactions, digital citizen services, and remote computer access, to cell phone calls and instant messaging. The vast majority of secured data sent over all types of networks is encrypted using so-called symmetric ciphers. The security of our digital infrastructure thus rests at its very base on their security.

The central topic of this thesis is the security of block ciphers – the most prominent form of symmetric ciphers. This thesis is separated in two parts. The first part is an introduction to block ciphers and their cryptanalysis, the second part contains publications written and published during the PhD studies. The first publication evaluates the security of a modification of the AES in which the choice of S-box is unknown to the attacker. We find that some of the attacks that can be applied to the AES can be transferred to this block cipher, albeit with a higher attack complexity. The second publication introduces a new block cipher family which is targeted for new applications in fully homomorphic encryption and multi-party computation. We demonstrate the soundness of the design and its superior performance in these applications. The third publication treats the cryptanalysis of Simon, a cipher proposed by the NSA. In particular we discuss how the methods of differential and linear cryptanalysis can correctly be applied to ciphers of this type. The fourth publication introduces a cryptanalytic framework which generalizes differential cryptanalysis. We demonstrate that attacks based on impossible transitions in this framework can competitively break round-reduced block ciphers in the low-data setting.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science
Contributors: Tiessen, T.
Number of pages: 151
Publication date: 2017

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
(DTU Compute PHD-2016; No. 412).
Electronic versions:
phd412_Tiessen_T.pdf
Research output: Research › Ph.D. thesis – Annual report year: 2017