Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48 - DTU Orbit (08/11/2017)

Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48

In this paper we analyse two variants of SIMON family of light-weight block ciphers against variants of linear cryptanalysis and present the best linear cryptanalytic results on these variants of reducedround SIMON to date. We propose a time-memory trade-off method that finds differential/ linear trails for any permutation allowing low Hamming weight differential/ linear trails. Our method combines low Hamming weight trails found by the correlation matrix representing the target permutation with heavy Hamming weight trails found using a Mixed Integer Programming model representing the target differential/linear trail. Our method enables us to find a 17-round linear approximation for SIMON-48 which is the best current linear approximation for SIMON-48. Using only the correlation matrix method, we are able to find a 14-round linear approximation for SIMON-32 which is also the current best linear approximation for SIMON-32. The presented linear approximations allow us to mount a 23-round key recovery attack on SIMON-32 and a 24-round Key recovery attack on SIMON-48/96 which are the current best results on SIMON-32 and SIMON-48. In addition we have an attack on 24 rounds of SIMON-32 with marginal complexity.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science , Cryptology, SICS - Swedish ICT, Sharif University of Technology, Shahid Rajaee Teachers Training University, Queensland University of Technology
Authors: Abdelraheem, M. A. (Ekstern), Alizadeh, J. (Ekstern), Alkhzaimi, H. A. (Intern), Aref, M. R. (Ekstern), Bagheri, N. (Ekstern), Gauravaram, P. (Ekstern)
Pages: 153-179
Publication date: 2015

Host publication information

Title of host publication: Progress in Cryptology – INDOCRYPT 2015 : Proceedings of the 16th International Conference on Cryptology in India
Publisher: Springer
Editors: Biryukov, A., Goyal, V.
ISBN (Print): 978-3-319-26616-9
ISBN (Electronic): 978-3-319-26617-6

Series: Lecture Notes in Computer Science
Volume: 9462
ISSN: 0302-9743
BFI conference series: INDOCRYPT (5010749)
Main Research Area: Technical/natural sciences
Conference: 16th International Conference on Cryptology in India, Bangalore, India, 06/12/2015 - 06/12/2015
SIMON, Linear cryptanalysis, Linear hull, Correlation matrix, Mixed Integer Programming (MIP), MIP
DOIs:
10.1007/978-3-319-26617-6_9
Source: FindIt
Source-ID: 2290358744
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015