Conditional differential cryptanalysis of 105 round Grain v1 - DTU Orbit (08/11/2017)

Conditional differential cryptanalysis of 105 round Grain v1

In this paper we propose conditional differential cryptanalysis of 105 round Grain v1. This improves the attack proposed on 97 round Grain v1 by Knellwolf et al at Asiacrypt 2010. We take the help of the tool ΔGrain K_{SA}, to track the differential trails introduced in the internal state of Grain v1 by any difference in the IV bits. We prove that a suitably introduced difference in the IV leads to a distinguisher for the output bit produced in the 105^{th} round. This helps determine the values of 6 expressions in the Secret Key bits. Using the above attack as a subroutine, we propose a method that determines 9 Secret Key bits explicitly. Thus, the complexity for the Key recovery is proportional to 2^{71} operations, which is faster than exhaustive search by 2^{9}.

General information

State: Published
Organisations: Cryptology, Department of Applied Mathematics and Computer Science
Authors: Banik, S. (Intern)
Pages: 113-137
Publication date: 2016
Main Research Area: Technical/natural sciences

Publication information

Journal: Cryptography and Communications
Volume: 8
Issue number: 1
ISSN (Print): 1936-2447
Ratings:

BFI (2017): BFI-level 1

Web of Science (2017): Indexed Yes

BFI (2016): BFI-level 1

Scopus rating (2016): CiteScore 1.13 SJR 0.412 SNIP 1.069

Web of Science (2016): Indexed yes

BFI (2015): BFI-level 1

Scopus rating (2015): SJR 0.585 SNIP 0.931 CiteScore 0.82

BFI (2014): BFI-level 1

Scopus rating (2014): SJR 0.824 SNIP 1.372 CiteScore 1.06

BFI (2013): BFI-level 1

Scopus rating (2013): SJR 0.974 SNIP 1.531 CiteScore 1.05

BFI (2012): BFI-level 1

Scopus rating (2012): SJR 0.544 SNIP 1.147 CiteScore 0.62

Web of Science (2012): Indexed yes

BFI (2011): BFI-level 1

Scopus rating (2011): SJR 0.288 SNIP 1.03 CiteScore 0.45

BFI (2010): BFI-level 1

Scopus rating (2010): SJR 0.385 SNIP 0.641
Original language: English
EStream, Differential cryptanalysis, Dynamic cube attack, Grain v1, Stream cipher
DOIs:

10.1007/s12095-015-0146-5
Source: FindIt
Source-ID: 2279552230
Publication: Research - peer-review › Journal article – Annual report year: 2016