# Cryptanalysis of Two Fault Countermeasure Schemes - DTU Orbit (08/11/2017)

## Cryptanalysis of Two Fault Countermeasure Schemes

In this paper, we look at two fault countermeasure schemes proposed very recently in literature. The first proposed in ACISP 2015 constructs a transformation function using a cellular automata based linear diffusion, and a non-linear layer using a series of bent functions. This countermeasure is meant for the protection of block ciphers like AES. The second countermeasure was proposed in IEEE-HOST 2015 and protects the Grain-128 stream cipher. The design divides the output function used in Grain-128 into two components. The first called the masking function, masks the input bits to the output function with some additional randomness and computes the value of the function. The second called the unmasking function, is computed securely using a different register and undoes the effect of the masking with random bits. We will show that there exists a weakness in the way in which both these schemes use the internally generated random bits which make these designs vulnerable. We will outline attacks that cryptanalyze the above schemes using 66 and 512 faults respectively.

### General information

State: Published
Organisations: Cryptology, Department of Applied Mathematics and Computer Science
Authors: Banik, S. (Intern), Bogdanov, A. (Intern)
Pages: 241-252
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
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
AES, Fault analysis, Grain-128, Infective countermeasures
DOIs:
10.1007/978-3-319-26617-6_13
Source: FindIt
Source-ID: 2290358558
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015