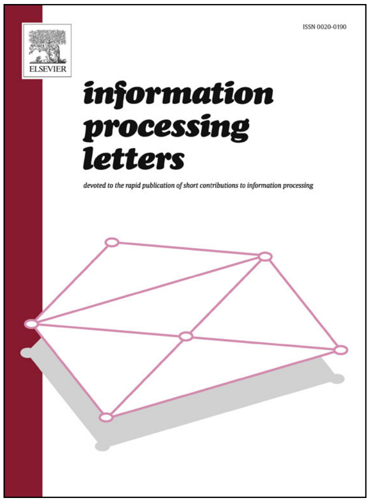
ISSN 0020-0190
ELSEVIER
information processing letters
devoted to the rapid publication of short contributions to information processing

Differential-linear and related key cryptanalysis of round-reduced scream

Ashutosh Dhar Dwivedi, Paweł Morawiecki, Rajani Singh, Shalini Dhar

PII: S0020-0190(18)30065-6
DOI: https://doi.org/10.1016/j.ipl.2018.03.010
Reference: IPL 5664

To appear in: *Information Processing Letters*

Received date: 23 November 2017
Revised date: 7 February 2018
Accepted date: 19 March 2018

Please cite this article in press as: A.D. Dwivedi et al., Differential-linear and related key cryptanalysis of round-reduced scream, *Inf. Process. Lett.* (2018), https://doi.org/10.1016/j.ipl.2018.03.010

Differential-linear and Related Key Cryptanalysis of Round-reduced Scream

Ashutosh Dhar Dwivedi[a], Paweł Morawiecki[a], Rajani Singh[b], Shalini Dhar[c]

[a]*Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland*
[b]*Institute of Applied Mathematics, University of Warsaw, Warsaw, Poland*
[c]*Sam Higginbottom Institute of Agriculture, Technology and Sciences, Allahabad, India*

Abstract

We have analysed tweakable block cipher Scream which is used by cipher SCREAM, with the techniques linear cryptanalysis, differential cryptanalysis and related key cryptanalysis. Tweakable block cipher Scream is already analysed with linear, differential-linear and impossible differential cryptanalysis in our previous paper. In this paper we extend our work by adding related key attack along with the differential-linear attack.

Keywords: Block Cipher, Linear Cryptanalysis, Differential Cryptanalysis, Tweakable Block Cipher, Related Key Cryptanalysis.

1. Introduction

Authenticated Encryption (AE) or Authenticated Encryption with Associated Data (AEAD) is a type of encryption that simultaneously provides integrity and confidentiality both, when passing the messages over an insecure channel. It encrypts and authenticates messages using both a secret key (shared by the sender and the receiver) as well as a public number (called a nonce). AE algorithms are often built as various combinations of stream ciphers, block ciphers, hash functions and message-authentication codes.

The great interest and importance of AE have been manifested by the announcement of a new public call for AE algorithms — the CAESAR competition [1]. The contest has started in 2014 and has received worldwide attention. CAESAR candidates are evaluated in terms of robustness, size, security, performance and flexibility. In the first round, 57 algorithms were submitted to CAESAR competition and SCREAM (Side-Channel Resistant Authenticated Encryption with Masking)[4] —the cipher we focus on, is one