How Not to Combine RC4 States - DTU Orbit (08/11/2017)

How Not to Combine RC4 States

Over the past few years, an attractive design paradigm has emerged, that aims to produce new stream cipher designs, by combining one or more independently produced RC4 states. The ciphers so produced turn out to be faster than RC4 on any software platform, mainly because the average number of internal operations used in the cipher per byte of keystream produced is usually lesser than RC4. One of the main efforts of the designers is to ensure that the existing weaknesses of RC4 are not carried over to the new ciphers so designed. In this work we will look at two such ciphers RC4B (proposed by Zhang et. al.) and Quad-RC4/m-RC4 (proposed by Maitra et. al.). We will propose distinguishing attacks against all these ciphers, and look at certain design flaws that made these ciphers vulnerable.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science , Cryptology, National Informatics Center
Authors: Banik, S. (Intern), Jha, S. (Ekstern)
Pages: 95-112
Publication date: 2015

Host publication information

Title of host publication: Proceedings of the 5th International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2015)
Publisher: Springer
Editors: Chakraborty, R. S., Schwabe, P., Solworth, J.
ISBN (Print): 978-3-319-24125-8
ISBN (Electronic): 978-3-319-24126-5

Series: Lecture Notes in Computer Science
Volume: 9354
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 5th International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2015), Jaipur, Rajasthan, India, 03/10/2015 - 03/10/2015
RC4, RC4B, Quad-RC4, m-RC4, Distinguishing Attacks, Stream Cipher
DOIs:

10.1007/978-3-319-24126-5_6
Source: FindIt
Source-ID: 2290010566
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015