Cryptology ePrint Archive: Report 2013/176

Distinguishing Attacks on RC4 and A New Improvement of the Cipher

Jing Lv and Bin Zhang and Dongdai Lin

Abstract: RC4, designed by Rivest in 1987, is the most widely deployed stream cipher in practical applications. In this paper, two new class of statistical biases inherent in RC4 are depicted and it is shown that the RC4 keystream is distinguishable from random no matter how many initial bytes have been dumped. RC4A, proposed by Paul and Preneel at FSE 2004 to strengthen the security of RC4, is also found to be vulnerable to similar attacks. Instead, a new pseudorandom bit generator RC4B is proposed, which is believed to provide better immunity against the known attacks.

Category / Keywords: secret-key cryptography / RC4, Bias, Distinguishing attacks, state

Date: received 27 Mar 2013

Contact author: lvjing at iscas ac cn

Available formats: PDF | BibTeX Citation

Version: 20130330:225125 (All versions of this report)