Cryptology ePrint Archive: Report 2013/096

State convergence in bit-based stream ciphers

Sui-Guan Teo and Harry Bartlett and Ali Alhamdan and Leonie Simpson and Kenneth Koon-Ho Wong and Ed Dawson

Abstract: Well-designed initialisation and keystream generation processes for stream ciphers should ensure that each key-IV pair generates a distinct keystream. In this paper, we analyse some ciphers where this does not happen due to state convergence occurring either during initialisation, keystream generation or both. We show how state convergence occurs in each case and identify two mechanisms which can cause state convergence.

Category / Keywords: secret-key cryptography / Stream ciphers, state convergence, Mickey, A5/1, Sfinks

Date: received 21 Feb 2013, last revised 21 Feb 2013

Contact author: teosuiguan at gmail com