Cryptology ePrint Archive: Report 2013/185

Security Analysis of Linearly Filtered NLFSRs

Mohammad Ali Orumiehchiha and Josef Pieprzyk and Ron Steinfeld and Harry Bartlett

Abstract: Our contributions are applying distinguishing attack on Linearly Filtered NLFSR as a primitive or associated with filter generators. We extend the attack on linear combinations of Linearly Filtered NLFSRs as well. Generally, these structures can be examined by the proposed techniques and the criteria will be achieved to design secure primitive. The attacks allow attacker to mount linear attack to distinguish the output of the cipher and recover its internal state. Also, we investigate security of the modified version of Grain stream cipher to present how invulnerable is the scheme against distinguishing attacks.

Category / Keywords: secret-key cryptography / Non-linear feedback shift register, Linearly Filtered NLFSR, Cryptanalysis, Key Recovery Attack, Distinguishing Attack.

Date: received 1 Apr 2013

Contact author: orumiehchi at gmail com