Available online at www.sciencedirect.com

SCIENCE DIRECT

Electronic Notes in Theoretical Computer Science

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Enhancements of a clock-controlled running key generator

Milan Vojvoda

Abstract

The design of stream ciphers based on the synthesis of linear feedback shift registers (LFSRs) has been the research target of many cryptographers for more than 50 years.

There is no general way for such a synthesis that results in design of a “secure” stream cipher. One of the design approaches is the use of basic design principles followed by properties testing procedures (system-theoretic approach).

In our contribution we present some enhancements of the generator studied in [6], [7]. The new designed generators consist of more LFSRs, use different clocking schemes and different output functions. We discuss their cryptographic properties and security against selected known attacks on stream ciphers.

10.1016/S1571-0661(05)80068-4