Cryptology ePrint Archive: Report 2011/632

A Scalable Method for Constructing Galois NLFSRs with Period 2^n-1 using Cross-Join Pairs

Elena Dubrova

Abstract: This paper presents a method for constructing n-stage Galois NLFSRs with period 2^n-1 from n-stage maximum length LFSRs. We introduce nonlinearity into state cycles by adding a nonlinear Boolean function to the feedback polynomial of the LFSR. Each assignment of variables for which this function evaluates to 1 acts as a crossing point for the LFSR state cycle. By adding a copy of the same function to a later stage of the register, we cancel the effect of nonlinearity and join the state cycles back. The presented method requires no extra time steps and it has a smaller area overhead compared to the previous approaches based on cross-join pairs. It is feasible for large n. However, it has a number of limitations. One is that the resulting NLFSRs can have at most $\lfloor n/2 \rfloor$-1 stages with a nonlinear update. Another is that feedback functions depend only on state variables which are updated linearly. The latter implies that sequences generated by the presented method can also be generated using a nonlinear filter generator.

Category / Keywords: foundations / NLFSR, LFSR, cross-join pair, stream cipher

Date: received 23 Nov 2011

Contact author: dubrova at kth se