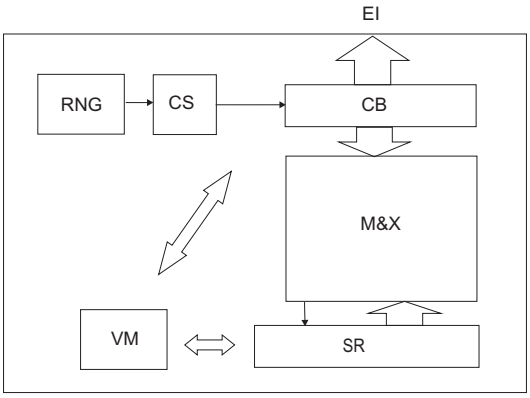
Generation of Nonlinear Feedback Shift Registers with special-purpose hardware

Tomasz Rachwalik, Janusz Szmidt,
Robert Wicik, and Janusz Zabłocki

Military Communication Institute
ul. Warszawska 22A, 05-130 Zegrze, Poland

Key words: Nonlinear feedback shift registers. Maximum period. Linear complexity. Hardware implementation. Randomness properties.

The nonlinear feedback shift registers (NLFSR) are used to construct pseudorandom generators for stream ciphers. Their theory is not so complete as that of the linear feedback shift registers (LFSR). In general, it is not known how to construct NLFSRs with maximum period. The direct method is to search for such registers with suitable properties. We used the implementation of NLFSRs in Field Programmable Gate Arrays (FPGA) to perform a corresponding search. We also investigated local statistical properties of the binary sequences ganerated by NLFSRs of order 25 and 27. It is calculated the linear complexity of NLFSRs of order 25 being $2^{25} - 2$.



A single module of the searching machine

The random NLFSR searching module (RNSM) consists of a random number generator (RNG), a coefficients selector (CS), a coefficients buffer (CB), multiplexers and XOR block (M&X), a shift register (SR), and a verification machine (VM). Random numbers are taken from the RNG. Coefficients are downloaded byte by byte into the CS, where their values and repetitions are controlled. Then the bytes go to the CB, whose task is to store combinations of coefficients during the test. The multiplexers define the feedback function of NLFSR according to the data buffered in the CB. Their outputs are connected to the XOR gate. Next, the output of the XOR function feeds the SR. The SR is set with a seed value at the beginning of a searching process by the VM and it starts to shift. After the first repetition of the seed the test is finished. A positive result is sent to the Ethernet Interface (EI), which is the same for all implemented modules. A negative result starts a new process of random generation and testing.
The NLFSRs of order 25 and 27:

$$f_{25}(x_0,\ldots,x_{24}) = x_0 + x_8 + x_9 + x_{10} + x_{11} + x_{19} + x_{20} + x_{21} + x_{23} + x_6x_{21} + x_{10}x_{14} + x_{12}x_{20} + x_{19}x_{20} + x_4x_{18}x_{21} + x_{11}x_{18}x_{22} + x_1x_5x_7x_{23}$$

$$f_{27}(x_0,\ldots,x_{26}) = x_0 + x_4 + x_8 + x_9 + x_{11} + x_{12} + x_{15} + x_{16} + x_{23} + x_{12}x_{22} + x_{13}x_{23} + x_{13}x_{25} + x_{22}x_{23} + x_7x_8x_{24} + x_{12}x_{14}x_{26} + x_6x_{11}x_{19}x_{22}$$

Reference: Tomasz Rachwalik, Janusz Szmidt, Robert Wicik, and Janusz Zabłocki. *Generation of Nonlinear Feedback Shift Registers with special-purpose hardware.* Cryptology ePrint Archive, 2012/314. www.iacr.org