ENHANCED CRYPTANALYSIS OF A CLOCK-CONTROLLED RUNNING KEY GENERATOR

Milan Vojvoda

Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Ilkovičova 3, 812 19 Bratislava, Slovak Republic
vojvoda@kmat.elf.stuba.sk

In our contribution we deal with further cryptanalysis of one simple running key generator presented in [1].

The generator consists of two clock-controlled linear feedback shift registers (CCLFSRs) - $L1$ and $L2$ respectively. The key sequence is produced as the bitwise XOR of outputs of $L1$ and $L2$. $L1$ and $L2$ are asynchronously clocked depending on the last produced bit of the key sequence.

According to [1] the cryptanalysed generator has a large linear complexity, is resistant against brute force and fast correlation attacks, but fails to a known plaintext attack.

In our contribution we study the number of runs in the maximum-length sequence and deal with the proof determining the period of the keystream (conjecture for a special case was formulated in [1]). The statistical properties of the keystream are studied, too.

In order to evaluate generated sequences we applied several statistical tests specified in FIPS 140-1, including gap test and serial correlation test. All of them passed the tests given by FIPS 140-1, but failed the gap test. 95% of them passed the serial correlation test.

Finally, a modification of the generator using substitution of FCSRs (feedback with carry shift registers) for CCLFSRs was studied, too. Neither this modification is resistant to a known plaintext attack presented in [1].

References

[1] Klapper, A., *Feedback with Carry Shift Registers over Finite Fields*, K.U.Leuven Workshop on Cryptographic Algorithms, Springer-Verlag 1995, p. 170-178..

[2] Menezes, A., van Oorschot, P., Vanstone, S., *Handbook of Applied Cryptography*, CRC Press 1996..

[3] Vojvoda, M., *Cryptanalysis of a clock-controlled running key generator*, Journal of Electrical Engineering 2000, No.10s, p. 16-19..