ON CONCATENATING PSEUDORANDOM SEQUENCES

Milan Vojvoda and Marta Šimovcová

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

The design goal in stream ciphers is to produce efficiently keystreams - pseudorandom sequences, i.e. sequences that possess features common for truly random sequences, and are in some sense "indistinguishable" from them [2], [3], [5].

There are some common cryptographic measures of their randomness, such as long period, large linear complexity, good autocorrelation property, and various statistical properties (uniform pattern distribution, etc.).

An approach to design of a completely equidistributed pseudorandom sequence based on concatenation of k-distributed sequences was given in [4]. Autocorrelation weaknesses in Ford's k-distributed sequence as well as in Knuth's sequence were observed in [6].

In our contribution we propose a construction of a completely equidistributed sequence based on concatenation of (almost k-distributed) ml-sequences. Next we study local properties of this sequence, namely concatenation of two ml-sequences. This part of our research was motivated by results on amplified weak-unpredictability obtained by concatenating the values of the function on several independent instances, see [1].

Analysis, using exhaustive computer simulations, shows that the concatenation of two ml-sequences has large linear complexity and moderate "out-of-phase" autocorrelation function magnitudes. It appears that concatenation of ml-sequences may bring interesting design ideas in the field of keystream generators.

References

[1] Goldreich, O., Nisan, N., Wigderson, A.: *On Yao's XOR-Lemma*, Electronic Colloquium on Computational Complexity Vol. 50, No. 2, 1995.

[2] Grošek, O.: *On the stability of stream ciphers (O stabilite prúdových šifier)*, Abstracts of the conference "Jesenný seminár z kryptoanalýzy", L.Mikuláš, October 9-11, 1996, pp.14-26, (in Slovak).

[3] Grošek, O., Nemoga, K., Satko, L.: *A remark to Luby-Rackoff and Ueli M. Maurer pseudorandom generators*, Abstracts of 14th Czech and Slovak International Conference on Number Theory, Liptovský Ján, September 6-10, 1999, pp. 1-4.

[4] Knuth, D.E.: *Construction of a random sequence*, Nordisk tidskrift for informationbehandling, Vol.5, No.4, 1965, pp. 246-250.

[5] Nemoga, K.: *Linear recurring sequences (Lineárne rekurentné postupnosti)*, Abstracts of the conference "Jesenný seminár z kryptoanalýzy", L.Mikuláš, October 9-11, 1996, pp.1-13, (in Slovak).

[6] Vojvoda, M., Šimovcová, M.: *Some properties of uniformly distributed sequences*, Abstracts of the conference "Elitech 2000", FEI-STU 2000.

This research was supported by VEGA-grant 1/7611/20.