PROPERTIES OF STREAM AND BLOCK CIPHERS - COMPARISON

MARTA ŠIMOVCOVÁ

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

Keywords: stream cipher, block cipher

There are many papers and books dealing with a research of stream ciphers e.g. [1],[2],[3],[4],[5]. Particularly they focus to algebraic and cryptographic properties of stream ciphers.

In this contribution we compare the main cryptographic characteristics of stream ciphers (like linear complexity, sphere complexity, autocorrelation properties and attributes of cyclotomic numbers) with properties of block ciphers.

The aim of this work is to find differences and similarities, and summarize advantages and disadvantages of the both types of ciphers.

REFERENCES

[1] O. Grošek, M. Zanechal: *Šifrovanie II*, Svet komunikácie, 1999, 24-26.

[2] G. Birkhoff, T. O. Bartee: *Aplikovaná algebra*, Alfa, Bratislava, 1981.

[3] B. Schneier: *Crypto-Gram*, http://www.counterpane.com/crypto-gram.html.

[4] R. Lidl, H.Niederreiter: *Introduction to finite fields and their applications*, Cambridge University Press,Cambridge, 1994.

[5] T. W. Cusick, C. Ding, A. Renvall: *Stream Ciphers and Number Theory*, Cambridge University Press, Cambridge, 1994.

Research supported by VEGA-grant 1/7611/20.