ABSTRACT

Vitruk I.V. Cryptanalysis of stream ciphers in high-performance computing systems

The thesis is submitted for the Master Degree in specialism 8.05010201 – Computer Networks and Systems. - Ternopil Ivan Pul'uj National Technical University, Ternopil, 2014.

Keywords: ANF, A5/1, CNF, Cryptominisat, DIMACS, DPLL, Grain of Salt, GSM, LFSR, SAT, NP-complete problem, cryptanalysis, algebraic cryptanalysis, cipher security, boolean functions, stream ciphers, linearization, high-performance computing, decomposition, XL-algorithm, copmuting clusters.

The work is dedicated to optimization of the stream ciphers cryptanalysis using the improved method of transformation of equations from ANF into CNF and by the usage of parallel-distributed problem solving methods, in particular, decomposition according to the data. Considering the wide usage of the stream ciphers and the existing modern methods of cryptanalysis, the methods for the effective investigation of well-known cryptographic stream ciphers are offered. Modern methods of cryptanalysis have been analyzed and the most appropriate and effective method – the algebraic cryptanalysis is selected. The mathematical apparatus for converting ANF into CNF is grounded and methods of optimization of such transformations are offered. Algebraic cryptanalysis high performance information system based on technologies and languages such as OpenMosix, Java, Prolog, Sat4J and, alternatively, Cryptominisat and Grain of Salt are elaborated. By usage of the designed system, cryptanalysis of the stream cipher A5/1 was done. Based on the conducted researches, recommendations for the improving of stream ciphers security and stability and their performing are formulated.