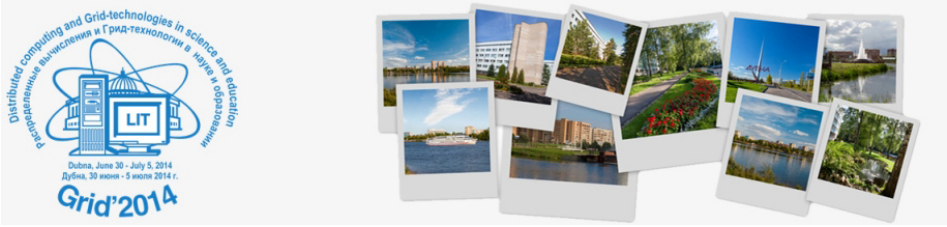

Contribution ID: **90** Type: **sectional reports**

Solving weakened cryptanalysis problems of Bivium cipher in the volunteer project SAT@home

Wednesday, 2 July 2014 17:30 (20 minutes)

A lot of important combinatorial problems (from areas of formal verification, planning, cryptology, etc.) can be effectively reduced to Boolean satisfiability problem (SAT). Despite remarkable progress in theory practical solving of many real-life SAT instances remains unmanageable on traditional PCs. Volunteer computing project SAT@home was launched to solve such hard instances.
Analysis of stream ciphers is quite important area of cryptology. Bivium stream cipher consists of 2 shift registers (93 and 84 cells). Below we use the notation BiviumK to denote a weakened problem for Bivium with known values of K variables (in corresponding SAT problem) encoding last K cells of the second shift register. We used computing cluster to find a variant of decomposition with good time estimations. An experiment based on this decomposition was lauhcned in SAT@home to solve weakened Bivium10 problems. During 3 months 3 problems were successfully solved. As far as we known there are no publicly available results of cryptanalysis of weakened Bivium problems.

Primary author: Mr ZAIKIN, Oleg (Institute for System Dynamics and Control Theory of Siberian Branch of Russian Academy of Sciences)

Co-authors: Dr SEMENOV, Alexander (ISDCT SB RAS); Dr POSYPKIN, Mikhail (ITTP RAS)

Presenter: Mr ZAIKIN, Oleg (Institute for System Dynamics and Control Theory of Siberian Branch of Russian Academy of Sciences)

Session Classification: Desktop grid technologies and volunteer computing

Track Classification: Section 7 - Desktop grid technologies and volunteer computing