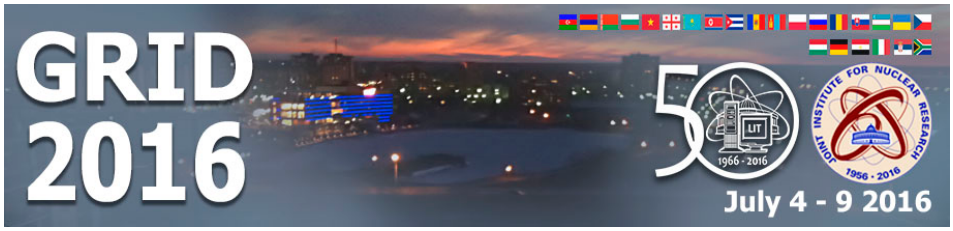

Contribution ID: **113** Type: **Sectional reports**

Using volunteer computing to solve SAT-based cryptanalysis problems for the Bivium keystream generator

Tuesday, 5 July 2016 16:15 (15 minutes)

Usually if the cryptanalysis is considered as a SAT problem then it is called a SAT-based cryptanalysis. In this case to find a secret key it is sufficient to find a solution of corresponding satisfiable SAT instance. Here we consider the SAT-based cryptanalysis of the Bivium keystream generator. This generator uses two shift registers of a special kind. The first register contains 93 cells and the second contains 84 cells. To initialize the cipher, a secret key of length 80 bit is put to the first register, and a fixed (known) initialization vector of length 80 bit is put to the second register. All remaining cells are filled with zeros. An initialization phase consists of 708 rounds during which keystream output is not released.
We considered cryptanalysis problems for Bivium in the following formulation. Based on the known fragment of keystream we search for the values of all registers cells (177 bits) at the end of the initialization phase. Therefore, in our experiments we used SAT encodings where the initialization phase was omitted.
The SAT-based cryptanalysis of Bivium turned out to be very hard, that is why we decided to solve several weakened cryptanalysis instances for this generator. Below we use the notation BiviumK to denote a weakened problem for Bivium with known values of K variables encoding the last K cells of the second shift register. In SAT@home 5 Bivium9 instances were successfully solved in 2014.
We also tried another approach for solving weakened Bivium instances. On the first stage a SAT instance is being processed on a computational cluster by running the PDSAT solver (which was developed by us) in the solving mode. During this process, the time limit equal to 0.1 seconds (this value was selected according to experiments) for every subproblem, is used. PDSAT collects (by writing to a file) all subproblems which could not be solved within the time limit. It turned out, that this approach allowed to solve 2 out of 3 instances Bivium10 on a cluster (i.e., despite the time limit, PDSAT found a satisfying assignments for these 2 instances). It should be noted, that during processing these 2 instances the new approach was about 2 times faster than the approach without time limits. Solving of the remaining instance was launched in SAT@home with the help of the file with data about the hard subproblems (interrupted by time limit), collected by PDSAT. Finally, this instance was successfully solved too. So, we can conclude that with the help of the proposed approach some instances can be quickly processed on a computational cluster, and a volunteer computing project suits well for processing the remaining instances. We hope that this approach will help us to solve nonweakened instances of cryptanalysis of Bivium in the nearest future.

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

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

Session Classification: 7. Desktop grid technologies and volunteer computing

Track Classification: 7. Desktop grid technologies and volunteer computing