Using BOINC Desktop Grid to Solve Large Scale SAT Problems

Mikhail Posypkin[1], Alexander Semenov[2], Oleg Zaikin[2]

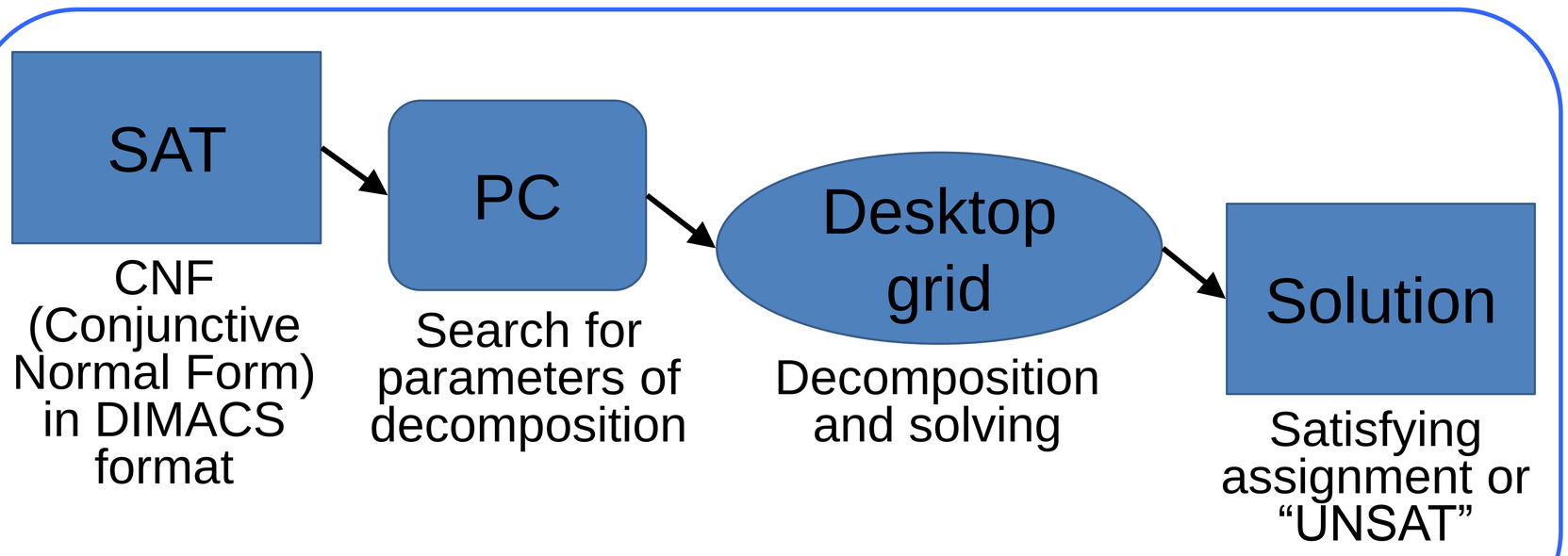
1. Institute for Systems Analysis of Russian Academy of Sciences, **mposypkin@gmail.com**
2. Institue for System Dynamics and Control Theory of Siberian Branch of Russian Academy of Science, **biclop@rambler.ru, zaikin.icc@gmail.com**

SAT@home is a research project that uses volunteer computing to solve hard and practically important problems that can be effectively reduced to Boolean satisfiability problem (SAT)

Problems being solved
Problems of inversion of some cryptographic functions (threshold, summation and A5/1 generators)

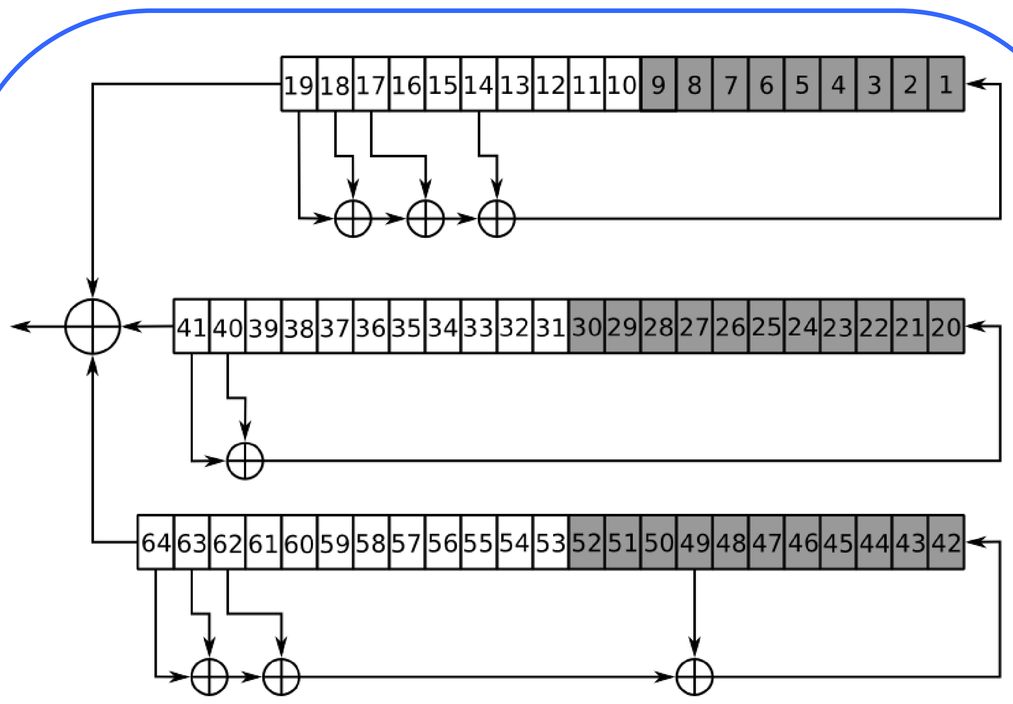
Applicability
- cryptography (experimental research of some stream ciphers, hash functions, etc.)
- discrete optimization (solving of some extremely hard optimization problems, like Quadratic Assignment Problem)
- bioinformatics (search of fixed points and attractors of discrete functions defining the dynamics of gene networks, like Kauffman networks)

General scheme for distributed solving of SAT problems in the project



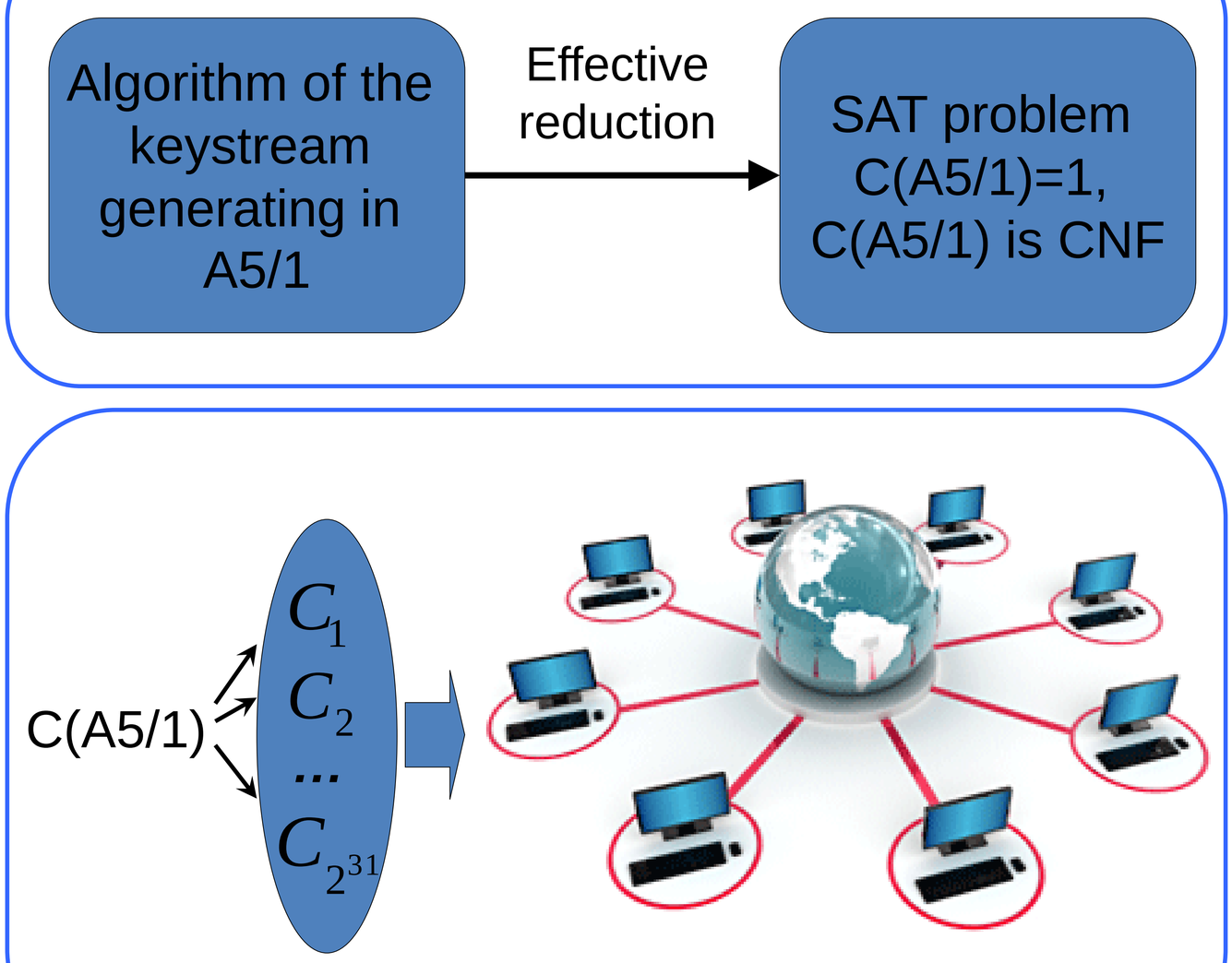
- CNF encoding of the original problem is decomposed into a set of CNFs
- For finding parameters of decomposition we use special technique of predictive functions
- We take into account peculiarities of the original problems

Example: Inversion of the generator A5/1



Scheme of the generator A5/1

- We use the decomposition set consisting of 31 Boolean variables which encode the initial state of the dark shaded cells
- Thus there are 2^{31} SAT problems to be solved in Desktop Grid



Desktop Grid

Implementation and the current state

Project was implemented using BOINC platform and DC-API library (http://www.desktopgrid.hu).

Client part of the application is based on SAT solver minisat (http://minisat.se) modified to take into account peculiarities of an original problem.

Launched : September 29, 2011,

Versions for client : windows and linux x86

State (October 31, 2011): **Teams** : 73. **Users** : 466. **Hosts** : 1046.

We would like to thank all the volunteers participating in the project!

SAT@HOME

Proud participant of IDGF

International Desktop Grid Federation | Supported by EDGI & DEGISCO | http://desktopgridfederation.org