Konstanty Junosza-Szaniawski
Warsaw University of Technology

Minimalization of Logic Formulas with Application in Cryptography

SAT-solvers continue to develop and they are able to solve bigger and bigger problems. Usually the shorter clauses are in CNF-form of SAT-formula the better solver can deal with it. Many problems can be encoded in different ways so natural question arises how to encode a problem into a SAT-formula in CNF-form such clauses are as short as possible.

We consider the problem of effective encoding of linear step of AES cypher. Given a homogeneous system of linear equations over field GF(2) we ask for an equivalent system with as short equations as possible (by a length of an equation we mean the number of non-zero coefficients). We can get an equivalent system by two operations: adding equations and by introducing new variable. We prove that the problem if a given linear system can be shorten to a system of equations with a given length is NP-hard. The problem has a nice combinatorial interpretation. Moreover we give some exact algorithm dedicated to this problem. Related problem was considered in [1].

This is joint work with Daniel Waszkiewicz.

References

[1] J. Boyar, P. Matthews, R. Peralta, *Logic Minimization Techniques with Applications to Cryptology*, Journal of Cryptology 26, 2013, pp. 280–312.