MINIMIZATION OF LENGTH OF SYSTEM OF LINEAR XOR EQUATIONS

Konstanty Junosza-Szaniawski

Warsaw University of Technology

e-mail: konstanty.szaniawski@pw.edu.pl

Daniel Waszkiewicz

National Institute of Telecommunications

e-mail: D.Waszkiewicz@il-pib.pl

SAT-solvers are one of the primary tools to assess the security of block ciphers automatically. A construction of a Boolean formula describing performance of a block cypher requires often an encoding a system of linear XOR equations over the field GF(2). Such systems are complex to write as MILP and requires many additional variables. If we model the system as CNF formula in a strait forward way the resulting formula contains many long clauses, which is not suitable for solvers. The standard procedure includes a greedy shortening algorithm is not always satisfactory. The problem of a straight-line program has been successfully applied in obtaining efficient implementations of MDS matrices [1, 2]. Inspired by this result, we consider the problem of minimization of the length of the linear equations XOR system. We can decrease a number of non-zero coefficient in a system by introducing new variables and by adding equations one to another.

The problem has a combinatorial formulation with hypergraphs. For a given hypergraph we want to reduce the maximum cardinality of an edge with two edge reductions. The question is how many operations we need. We show NP-hardness of the problem and give some algorithm solving it.

References

[1] J. Boyar, P. Matthews, and R. Peralta. Logic minimization techniques with applications to cryptology. J. Cryptol., 26(2) 280-–312, (2013).

[2] T. Kranz, G. Leander, K. Stoffelen, and F. Wiemer. Shorter linear straight-line programs for mds matrices. IACR Transactions on Symmetric Cryptology, (4) 188-–211, Dec. (2017)