Hill climbing algorithms and trivium

This paper proposes a new method to solve certain classes of systems of multivariate equations over the binary field and its cryptanalytical applications. We show how heuristic optimization methods such as hill climbing algorithms can be relevant to solving systems of multivariate equations. A characteristic of equation systems that may be efficiently solvable by the means of such algorithms is provided. As an example, we investigate equation systems induced by the problem of recovering the internal state of the stream cipher Trivium. We propose an improved variant of the simulated annealing method that seems to be well-suited for this type of system and provide some experimental results.

General information
State: Published
Organisations: Discrete mathematics, Department of Mathematics
Contributors: Borghoff, J., Knudsen, L. R., Matusiewicz, K.
Number of pages: 410
Pages: 57-73
Publication date: 2011

Host publication information
Title of host publication: Lecture Notes in Computer Science
Volume: 6544
Publisher: Springer
Keywords: Cryptanalysis, Trivium, Simulated annealing
DOIs: 10.1007/978-3-642-19574-7_4
URLs: http://sac2010.uwaterloo.ca/
Source: orbit
Source-ID: 278321
Research output: Research - peer-review » Article in proceedings – Annual report year: 2011