UNIVERSITY OF BAHRAIN
College of Information Technology

Automated Design of Stream Cipher Using
GADS and Simulated Annealing

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Master Degree in Information Technology

Submitted by
Amal Mohammed Al Hiddi
University number: 19991154

Supervised by
Wasan Shaker Awad
(Associate professor)
University of Bahrain

Kingdom of Bahrain
December, 2014
Abstract

Stream cipher is important method in encryption for many reasons such as security level, easy to implement and efficient (in terms of space and time). The mechanism of how stream cipher work is that cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.

The main objective of this thesis is to propose a new effective algorithm to design stream cipher systems automatically using genetic programming with different representation method for representing the genetic programming population individuals compare with simulated annealing algorithm. Usually the individual programs of genetic program population represented using LISP expressions. In the proposed method, the programs are represented as strings of integers representing the individual program syntactic rule numbers. This representation method is called genetic algorithm for developing software (GADS). The performance of the proposed algorithm is studied by applying different genetic parameters and methods such as selection algorithm, crossover and mutation. Furthermore, it is compared with other representation methods such as LISP expression.