Chapter 3
Automated Design of Stream Ciphers Using GADS

Wasan Shaker Awad
Ahlia University, Bahrain

Amal M. Al Hiddi
University of Bahrain, Bahrain

ABSTRACT

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

INTRODUCTION

Nowadays, in the organizations, there is a great dependence on information, computer systems, and computer communication and networking. Consequently, awareness of the need to security has been also increased. Information security is the process of protecting information from unauthorized access, use, disclosure, destruction, or modification. The organizations need to protect information from malicious actions that endanger the confidentiality of its information, such as snooping and traffic analysis. There are a number of information security goals, one of them is confidentiality. It is about protection of confidential information.

Encryption is an important mechanism used to protect information. Therefore, we can see many encryption techniques proposed with different levels of security, and different structures. One of encryption systems is stream cipher which is an important class for many reasons, such as security degree, easy to implement, efficient, and with no error propagation.

DOI: 10.4018/978-1-4666-9426-2.ch003

Designing cipher systems of good characteristics, such as security level, efficiency, and ease of implementation, is hard task. Therefore, this problem has attracted a number of researchers, and some of them proposed automated methods for designing cipher systems. In this chapter, we are trying to find an efficient and effective automated method for designing cipher systems, to help the security researchers and industry to find strong cipher systems. The proposed method for designing cipher systems is based on genetic programming (GP), which is an application of genetic algorithm (GA). GP has been used to solve different kinds of problems, and attracted many researchers. Thus, we can find so many studies about applying GP to solve complex problems, and most of studies proved its effectiveness. Thus, this work is to study the effectiveness of GP in designing stream ciphers automatically. In the literature, we can find different studies about the automated design of cipher systems using computational intelligence techniques (CI). Awad (2011a, 2011b, 2013) proposed a different variations of GP-based stream cipher design algorithm, such as adaptive GP and simulated annealing programming. This chapter is to present a modified SAP algorithm using GADS.

Although GA (and GP) has gained many applications, simple GA suffers from many troubles such as getting stuck in a local minimum and parameters dependence (Eiben, Hinterding, & Michalewic, 1999). There are many improvements have been proposed to enhance the performance of the GA. Therefore, in this work, to avoid the problem of getting stuck in a local minimum and to preserve good individuals into the next generation, simulated annealing algorithm (SA) is integrated with GP, the resulted algorithm is called simulated annealing programming (SAP).

The main objectives of this chapter are:

1. Study the effectiveness of GP in the automated design of stream cipher systems of high level of security.
2. Analyze the application of GP with GA engine, i.e., genetic algorithm for developing software (GADS).
3. To study the effect of different GA techniques and parameters on the performance of GP-based design method.

In the next three sections, the concepts of stream ciphers, GP, and SA are given. The sections after are for describing the proposed method, architecture, algorithms, and experimental results.

STREAM CIPHER

Cryptology is the study of the encryption techniques to protect data and the techniques to attack the encryption techniques. Thus it is combination of two areas: cryptanalysis and cryptography, where cryptanalysis is the study of the techniques used for breaking cryptographic (cipher) systems, and cryptography is the science of encrypting information. There are different kinds of cipher systems (cryptosystems), used for encrypting the private information. The cryptosystems can be classified into modern and classical systems. Modern cipher systems are subdivided into block ciphers and stream ciphers (Paar, and Pelzl, 2010).

Stream ciphers are extremely fast and easy to implement, in addition, they usually have very minimal hardware resource requirements. Therefore stream ciphers are of great importance in applications where encryption speed is paramount and where area-constrained or memory constrained devices make it im-