Chapter 6
Cryptographic Techniques Based on Bio-Inspired Systems

Petre Anghelescu
University of Pitesti, Romania

ABSTRACT

In this chapter, bio-inspired techniques based on the cellular automata (CAs) and programmable cellular automata (PCAs) theory are used to develop information security systems. The proposed cryptosystem is composed from a combination of a CA as a pseudorandom number generator (PRNG) and a PCA that construct the ciphering functions of the designed enciphering scheme. It is presented how simple elements named „cells" interact between each other using certain rules and topologies to form a larger system that can be used to encrypt/decrypt data sent over network communication systems. The proposed security system was implemented in hardware in FPGA devices of type Spartan 3E – XC3S500E and was analyzed and verified, including NIST statistical tests, to assure that the system has good security and high speed. The experimental results proves that the cryptographic techniques based on bio-inspired algorithms provides an alternative to the conventional techniques (computational methods).

INTRODUCTION

Because the communications and computer systems become each time more pervasive, cryptographic techniques plays an essential role, requiring new solutions, in order to provide *data authentication*, *integrity* and *confidentiality* in insecure environments. The interconnection of these pervasive devices leads to Mark Weiser's famous vision of ubiquitous computing (Weiser, 1999) and in this way within any minute, a huge amount of information is exchanged through the Internet or over other insecure communication channels. Many kinds of information exchanges, for example text, audio/video content, in multimedia communications, should be protected from *unauthorized copying*, *intercepting* and *tampering* as they are traversing on public digital networks. Accordingly, cryptography has become more important in data security. Also, in the recent years, researchers have remarked the similarities between bio-inspired systems (particularly cellular automata), chaos and cryptography (Dachselt, & Schwarz,

DOI: 10.4018/978-1-7998-1763-5.ch006

2001; Fuster-Sabater, & Cabalerro-Gil, 2010; Kocarev, & Lian, 2011). Some of the cellular automata features as *ergodicity* and *sensibility to the initial conditions* and *control parameters* can be correlated with the cryptographic properties as *confusion* and *diffusion*.

The essence of the theoretical and practical efforts which are done in this new field is represented by the idea that bio-inspired based encryption techniques are capable to have similar performances regarding the classic methods based on computational techniques. In this paper is presented an encryption system that uses a combination of two cellular automata*: a first class of cellular automaton* that generates the evolution rules for the second class of *five programmable cellular automata* arranged in pipeline. The entire security system was implemented both in software using C# programming language and in hardware on a FPGA of type Spartan 3E – XC3S500E in which the plaintext/ciphertext is received/transmitted using User Datagram Protocol (UDP).

This chapter is organized in eight sections. In the *background section*, are described some basic theoretical foundations of the proposed work that includes CAs and PCAs. The *third section*, provides a brief overview of the classical cryptography and bio-inspired systems in cryptography. The *next section*, on *reconfigurable hardware devices*, introduces the existing reconfigurable hardware devices approaches for supporting bio-inspired algorithms and presented also the reasons for using them in the application presented in this chapter. Then, the section *bio-inspired based algorithm for cryptography*, describes the proposed bio-inspired encryption algorithm used to encrypt and decrypt data sent over the communication networks. Additionally, in section *testing and experimental results*, are made the investigations of statistical properties of the encrypted sequences (performed using NIST statistical tests), distribution of text (plaintext and ciphertext) and encryption/decryption speed. In the next section, are presented the future research direction of the research presented in this chapter. Finally, section eight, conclude the chapter.

BACKGROUND

The intersection of biology and computer science has been a productive field for some time. On one hand, CAs is a bio-inspired paradigm highly addressing the soft computing and hardware for a large class of applications including information security. On the other hand, PCAs is a modified CAs structure including switches in order to allow the self-organizing of the cellular structure.

Cellular Automata (CA)

CAs, first introduced by von Neumann and Stanislav Ulam (Neumann, 1966) in the ‘50s, exhibit useful and interesting characteristics and has attracted researchers from different field of interests, who applied it in different ways. The most notable characteristics of CAs are: *massive parallelism*, *locality of cellular interactions* and *simplicity of basics components*. CAs perform computations in a distributed way on a spatial grid and differ from a standard approach to parallel computations whereby a problem is split into independent sub-problems later to be combined in order to yield a final solution. CAs suggest a new approach in which a complex global behavior can be modelled by non-linear spatially extended local interactions.

Thus far, CAs have been used primarily to model the systems consisting of a number of elements obeying identical laws of local interactions (e.g. problems of fluid dynamics, plasma physics, chemical systems, crystals growth, economics, two-directional traffic flow, image processing and pattern recognition,