Abstract

This document presents an overview of my research work in the last ten years, i.e. after I finished my PhD thesis in December 2007. The PhD. Thesis was certified by the Ministry of Education, Research and Youth, Order No. 3439/12.03.2008.

I consider this habilitation thesis as an opportunity to provide additional hindsight and overview to my works over the past 10 years. Rather than duplicating previously published papers – which would be somewhat redundant and not so interesting – I will try to provide the global picture, revealing the strong links between the different publications and projects realized. There will be fewer details than in each of the publications, because I will rather focus on what I think, in hindsight, are the most important ideas.

In accordance with the current regulations, the first section of this habilitation thesis, beyond this abstract, is represented by the author's scientific, professional and academic achievements, on disciplinary or interdisciplinary thematic directions. A description of this part, consisting of four chapters, is given below.

Generally, my research activity that concerns the fundamental and interdisciplinary aspects in the area of great sensitivity – artificial intelligence (cellular evolutionary computing algorithms) & data protection – can be divided and certified into two important directions, i.e. the teaching and publishing activity and the actual research activity, respectively.

In the first direction, in chapter one, I have mentioned my teaching career which was started in 2002 at the Faculty of Electronics, Communications and Computers of the University of Pitesti and continues up to this day, as well as the activity as a member in the supervising committees of the PhD. students.

In the second direction, I have presented the most important achievements (what I found worthy to be mentioned) related to the major research fields mentioned above (scientific articles, research projects won in the competitions as project director, patent, project at the NKS summer

school, joint with the industry, and so on). My scientific research activity has been conducted mainly in the fields of artificial intelligence – cellular automata & cryptography, through exploring the possibility of using cellular automata for processing of the information stored or transmitted in telecommunication networks.

In chapter two, the research has been justified by the fact that in the recent years the need for protection by encryption of a large amounts of data stored or transmitted through communication networks is increasingly more stringent. On one hand, this modern society depends on cryptography and it could not maintain its current operations without the protocols based on cryptosystems. On the other hand, currently there is no infallible cryptographic strategy and this representing an additional reason on the development of new methods and cryptosystems. In this context, the development of cryptosystems that uses new techniques and technologies, able to offer a degree of safety at least equal to the classical methods (computational), is a major research direction. The main idea was to use the structural similarity between the cellular automata and programmable cellular automata (*parallel computer systems – without central processing unit*) and natural systems (*nature was and will remain for the scientists, both the major challenge and the main source of inspiration*) made of a great number of simple components which interact locally (*the system's macroscopic evolution being in fact the reflection of the microscopic evolution*) in the development of new cryptosystems at a low cost, high operating speed and advanced security.

I have shown that the cellular automata and programmable cellular automata design methods may, in some cases, provide innovative results through exploring the places in the search space that are unreachable by the traditional approaches. Therefore, it is needed to investigate not only the solutions obtained but also the ways how to create the solutions. In this way, taking into account the great potential of using cellular automata concepts in cryptography, we can obtain knowledge that can enrich our understanding of cellular evolutionary engineering methods and enable us *to invent new and innovative cryptosystems*.

Further, in chapter three, we discussed about the design of original applications of the cellular automata and programmable cellular automata in the field of cryptography. The encryption/decryption methods described there are mainly based on the features of two types of cellular automata: a pseudo-random number generator with very good statistic properties and

programmable cellular automata with multiple transformations applied to the original message.

In chapter four, I provide the technical details of the most representative results and I have described my contribution and the arguments that demonstrate the ability of cellular automata and programmable cellular automata based algorithms to combine the two necessary properties *diffusion* (*sensibility to the initial conditions and control parameters*) and *confusion* (*ergodicity property of some cellular automata classes*) in order to obtain very good cryptographic solutions.

The second section of the thesis, presented in chapter five, outlines future research plans that include both education and research.

The third section (final part) contains the references that include my scientific publications and general publications that were used in the first two sections.

Date:
Pitesti, 19.06.2017

Associate Professor PhD. Eng.
Petre ANGHELESCU