resulting path; the keys of the cryptosystem are the states of the CA and PCA, the evolution rules used and the number of evolution steps.

Development of new encryption techniques based on PCA implies a huge simulation effort in order to choose a number of local rules, combined with appropriate initial states and topology, which can be effectively applied in cryptography.

The encryption/decryption modules share the same structure, so it is easy for implementation (also in hardware). Because of the nature of the CA, the encryption algorithm is most efficient when implemented in massively parallel integrated circuits (FPGA).

In the immediate future, the PCA encryption project will be implemented in hardware, in FPGA circuits, to achieve *high speed* (specialized hardware has a significant performance advantage) and *good security* (there is no physical protection for an encryption algorithm written in software).

6. Acknowledgements

This work was supported by CNCSIS/CNCS UEFISCSU/UEFISCDI, project number PN II-RU PD 369/2010, contract number 10/02.08.2010.

7. References

[1] S. Wolfram, *A new kind of science*, Wolfram Media Inc., ISBN: 1-57955-008-8, 2002.

[2] O. Lafe, *Cellular Automata transforms: theory and applications in multimedia compression, encryption and modelling*, Kluwer Academic Publisher, 2000.

[3] J. von Neumann, *Theory of Self -Reproducing Automata*, edited and completed by Burks, A.W. (Ed.), Univ. of Illinois Press, London, 1966.

[4] S. Wolfram, *Theory and Application of Cellular Automata*, World Scientific, 1986.

[5] S. Nandi, B. K. Kar, P. P. Chaudhuri, "Theory and applications of cellular automata in cryptography". *IEEE Transactions on Computers*, 43(12):1346-1356, 1994.

[6] F. Schweitzer, J. Zimmermann, "Communication and self-organization in complex systems: A basic approach", *Knowledge, Complexity and Innovation Systems*, 275-296, 2001.

[7] P. D. Hortensius, R. D. McLeod, B. W. Podaima, "Cellular Automata Circuits for Built-in Self-test", *IBM J. RES. DEVELOP.*, Vol. 34, No.2/3, pp. 389-405, 1990.

[8] P. Anghelescu, S. Ionita, E. Sofron, "Encryption Technique with Programmable Cellular Automata (ETPCA)", *Journal of Cellular Automata*, ISSN 1557-5969, Volume 5, Issue 1-2, 2010.

[9] S. Ionita, P. Anghelescu, S. Puscoci, M. Ionita, "The patient home assistance application based on telemedicine service", *Med-e-Tel 2007*, pp. 376-379, Luxembourg, 18-20 April 2007.

[10] A. Rukhin, J. Soto, J. Nechvatal1, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, "A Statistical Test Suite for Random and PseudoRandom Number Generators for Cryptographic Applications", *NIST (National Institute of Standards and Technology) Special Publication 800-22*, (2005&2010), http://csrc.nist.gov/rng/.

