Encryption with two-dimensional cellular automata

Abstract

The goal of this dissertation is to present a new symmetric block cipher called 2DCARotate, based on two-dimensional cellular automata and certain non-affine rotations of squares. This cipher is characterised by a simple construction that can be implemented as simple logic circuit. The specific cellular automata used, and carefully selected non-affine geometric rotations provide an easy way to parallelize the processing (encryption and decryption), due to which this cipher with the proper implementation gets very efficient.

The novelty of this study is, first of all, the application of three two-dimensional automata to encrypt data. It is not one automata, but three automata cooperating with one another for the data processing purpose. The operations of the automata rules are reversible and irreversible transformations, which is also a novel solution used with the two-dimensional automata. Another innovative element included in the design of the 2DCARotate cipher is the use of certain geometric transformations ~~based~~ on squares. These transformations, apart from the fact that they are characterized by a high nonlinearity, were chosen in such a way that they can be performed in parallel. By combining the two-dimensional cellular automata with the aforementioned geometric rotations, we have obtained a hybrid cipher, characterized by good quality ciphertexts, as well as high performance throughput and ease of implementation.

An important part of this dissertation is the implementation of this cipher (in addition to the PC implementation) for the FPGA-type[1] digital circuit using a hardware description language VHDL[2] and Quartus II 9.0 Web Edition toolkit[3]. The aim of this was to demonstrate the hardware high performance of 2DCARotate cipher, so that one can compare it to the hardware implementations of well-known cryptosystems, for example DES, 3DES, AES-Rijndael. Thanks to the massive parallel processing provided by cellular automata and the discussed square rotations, very promising results have been obtained.

At this point other assumptions should also be mentioned that were the motivations for the construction of 2DCARotate. One of the important objectives was to design a hybrid cipher and apply cellular automata as parallel architecture. As usual in such situations, a family of ciphers was actually obtained. A specific code has been determined by choosing the parameters (e.g. the key length).

The design of a cipher was the main objective of this thesis, but not the only one. Each new cipher should be examined with regard to the possibility of attacks on it with various currently known techniques. Ciphers of good quality should resist such attacks. Therefore, the thesis presents the statistical tests to verify quality of the cipher, and some results on its security. The thesis contains the results on nonlinearity of the 2DCARotate algorithm that provide reasonable hope of the cipher resistance to the linear cryptanalysis. The possible attack with differential cryptanalysis is also countered.

[1] FPGA (Field Programmable Gate Array) is a kind of programmable logic system, which can be repeatedly reprogrammed by the user in the purchased target device (e.g. washing machine, fridge, MP3).

[2] Very High Speed Integrated Circuits Hardware Description Language is the language of specification and description of the hardware used for computerized design of digital circuits.

[3] Altera Quartus II Web Edition Software, http://www.altera.com/products/software/quartus-ii/web-edition/qts-in-index.html. Retrieved 02.02.2013.