Block Cipher Based on Reversible Cellular Automata

Marcin SEREDYNSKI and Pascal BOUVRY
Faculty of Science, Technology and Communication,
University of Luxembourg
6, rue Coudenhove Kalergi,
L-1359, Luxembourg-Kirchberg, Luxembourg
{marcin.seredynski,pascal.bouvry}@uni.lu

Received 30 March 2004
Revised manuscript received 7 July 2004

Abstract We propose a new encryption algorithm relying on reversible cellular automata (CA). The behavior complexity of CA and their parallel nature makes them interesting candidates for cryptography. The proposed algorithm belongs to the class of symmetric key systems.

Keywords: Cryptography, Reversible Cellular Automata, Block Ciphers.

§1 Introduction

Considering the fast development of network computing, information security becomes increasingly important. One of the principal requirements for network and communication security is confidentiality (privacy). Its goal is to keep information secret from all but those authorized to access it. Demand for confidentiality can be satisfied by the means of various encryption techniques.

By applying an encryption algorithm to a message, it becomes scrambled and unreadable as is. In order to decrypt the message some secret information (called key) is required. Encryption techniques are divided into two groups referred as symmetric-key and public-key techniques. If both the sender and the receiver use the same key, or it is easy to deduce one key from the other then the system is referred to as symmetric-key encryption. If the sender and receiver use different keys, and if it is computationally infeasible to determine one from the other without knowing additional (secret) information then the system is referred to as a public-key encryption. There are two classes of symmetric-key encryption schemes: block ciphers and stream ciphers. A block cipher breaks up the message into fixed length blocks and encrypts one block at a time. A stream cipher encrypts one bit at a time.
Cellular Automata (CA) were invented in the 1940's by the mathematicians John von Neumann and Stanislaw Ulam. They are dynamical systems which are discrete in space and time. Their behavior is characterized by simple “local” interactions. Despite the simplicity of the interactions, an impressive diversity of behaviors is achieved. Some of the CA are reversible which means that the processed information is preserved. CA have been applied for symmetric-key and public-key cryptography. A CA-based public-key cipher was proposed by Guan.\(^3\) The security of this algorithm is based on the difficulty of solving a system of nonlinear polynomial equations. A stream CA-based encryption algorithm was first proposed by Wolfram.\(^8\) The idea behind this algorithm is to use CA for generating pseudo-random numbers. Then generated sequences were combined using exclusive-or (XOR) operation with the plaintext in order to produce the ciphertext. The proposed secret key consists of the initial state of CA. For the decryption the same pseudo-random sequence must be re-generated (using the secret key and the CA) and then re-combined with the ciphertext. This algorithm was later developed by Tommassini et al.,\(^5\) and recently by Seredyński et al.\(^4\) A block cipher using both reversible and irreversible rules was proposed by Gutowicz.\(^9\)

In this article we present a new symmetric-key block cipher based on a specific class of reversible CA.

§2 Encryption Using Symmetric-key Algorithms

The symmetric-key encryption scheme is shown on Fig. 1. It is composed of five elements: plaintext, encryption algorithm, ciphertext, decryption algorithm and key. Plaintext is the original message that is going to be encrypted. The encryption algorithm describes the operations to be performed on the plaintext. As a result of the encryption a scrambled message called ciphertext is produced. The exact transformations performed on the plaintext during encryption are defined by the key. Changing the key will result in a different ciphertext produced by the algorithm. To convert ciphertext into plaintext a decryption algorithm is used. It takes as input the ciphertext and the key. Usually decryption algorithms consist of running the encryption algorithm in the reverse order.

A first important property of good encryption algorithms is called the avalanche property that implies that a small change in either plaintext or in