World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 270-273, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.csea.2257

Symmetric Key Cryptosystem Using 2d Reversible Cellular Automata

V. Khanaa, K.P. Thooyamani and R. Udayakumar

School of Computing Science, Bharath University, Chennai-73, India

Abstract: Traditional 2-dimentional reversible cellular automata (2-D RCA) is fit for cryptography for its rules being an affine function, i.e.. . . two reversible CA's rules can be applied in encryption process while another counterpart rules can be applied in decryption process In this paper, a 2- D RCA is proposed aimed to be applied in cryptography.

Key words: Cellular automata · 2-dimensionsional cellular automata · Encryption · Decryption

INTRODUCTION

With developing of progress and civilization more techniques of cryptography was discovered and improved because, the interest in hiding electronic messages has grown up. The main aspect of information is security, privacy, data integrity, authentication and non-repudiation. Cryptographic techniques, which is one of the effective methods for protecting the private data, has attracted more attention[1].

Cellular automata (CA) have been considered for application in cryptography ever since they appeared. CA has the characters of simplicity and regularity of basic components, locality of cells, interactions, massive parallelism of information processing and exhibits complex global properties, which make it suitable for application in cryptography [2, 3]. Cellular automata were introduced by J.Von Neumann and S. Ulam. They are discrete dynamical system formed by a finite number of memory units called cells endowed with a state at every step of time. These states change accordingly to a local transition function taking into account the interaction between the neighbour cells. These simple state machines are capable to simulate complex physical, biological or environmental phenomena [4].

The use of cellular automata to design cryptographic protocols goes back to middle eighties when Wolfram proposed the cellular automaton with rule number 30 as a pseudorandom bit generator for cryptographic purposes. Since then, many cryptosystems based on cellular automata have been proposed [5].

This paper deals with confidentiality [1]. Our main goal is to provide an efficient mathematical algorithm to enable two people to communicate over an insecure channel in such a way that an opponent cannot understand what is being said. To get this objective, the original message to be sent (plaintext) must be modified, according to an algorithm (cryptosystem) and some parameters called keys, to obtain the encrypted message (cryptogram). If the keys are only known for the sender and the receiver of the message, the cryptosystem is called symmetric or secret-key cryptosystem and its security mainly relies on keeping secret the key used. On the other hand if the key to encrypt the message (public key) is publicly known, whereas the key to decrypt the message (secret key) is only known by the receiver, the cryptosystem is called asymmetric or public key cryptosystem [1].

In this work we are interested in the use of a very simple computational model, called reversible memory cellular automata(RCA), in order to design a secret key cryptosystem (block cipher). This traditional RCA could be used in public-key cryptographic algorithm; however, the RCA cannot satisfy the large key space demand since there are only small quantities of RCA in primary CA [6]. For example, there are only six reversible rules in elementary CA.

In this paper, a simple method to construct RCA is proposed. This extended RCA is based on ordinary CA and CAM. Unlike the traditional RCA, the extended RCA has a large number of reversible rules which meet the basic demand of cryptography. Based on the RCA, a block data cryptographic algorithm is proposed [7].

Corresponding Author: V. Khanaa, School of Computing Science, Bharath University, Chennai-73, India.

The paper is organized as follows: Section 2 point out general concepts of CA, 2-D CA and RCA. The idea on how the RCA can be used in cryptography is also presented in this section. Section 3 presents the detail of encryption model based on 2-D RCA.

Preliminaries

Cellular Automata: A cellular automaton is a discrete dynamical system. Space, time and the states of the system are discrete. Each point in a regular spatial lattice, called a cell, can have any one of a finite number of states. Considering the convenience to be treated by computer, many researchers only considered every cell only has two states $c_i \in \{0,1\}$. The state of a cell at the next time step is determined by the current states of the surrounding neighbourhoods,

$$\text{i.e. } c_i^{j+1} = f(c_{i-r}^j, c_{i-r+1}^j \ldots c_i^j, c_{i+1}^j, \ldots, c_{i+r}^j)$$

where r is the neighbourhood radius, c_i^j means the state of the i^{th} cell at time j. All cells on the lattice are updated synchronously. Thus the state of the entire lattice advances in discrete time steps. Since the transition rule is simple, local and discrete, it can be executed in easily-constructed and massively-parallel hardware at extraordinary speeds, without round-off errors. The simplest cellular automaton is elementary cellular automata (ECA) whose rule radius r is 1 and every cell only has two states (0 and 1). The transition rule f of elementary cellular automata is:

$$c_i^{j+1} = f(c_{(i-1+n) mod n}^j, c_{(i+1+n) mod n}^j)$$

c_i^j means the state of the i^{th} cell at time j. The cellular array is
d-dimensional, where $d = 1, 2, 3$ is used in practice

Reversible Computation: Any reversible computation, whether performed by a slide rule, computer work station or brain, is inherently a physical process and as such is subject to whatever laws and limitations apply to physical system in general. It is natural question to ask, then, whether there exists a thermodynamic limit to the computation i.e. whether there is a minimum amount of energy that is required to perform a given logical operation? [8].

A CA is reversible if and only if the transition rule f is one-to-one that is if every configuration not only has one successor but also has one predecessor. According to the property, after a CA using a reversible rule to take n steps iteration, another counterpart rule can be applied the same iterations to obtain the original configuration of the CA. For example, after 5 iterations by rule 170, the CA can recede to the original state by rule 240. Reversible rules that could be useful in cryptography should meet the following criteria: they should be numerous and they should exhibit complex behaviour. When analyzing elementary CA it turns out that only a small number of rules have the property of being reversible. For example, among all 256 radius 1 CA there are only six reversible CA. This is why class of CA with rules specially created to be reversible is considered.

In 1997, Toffoli proposed a novel class CA which called cellular automata with memory (CAM). In CAM, the state of cell depends not only depends on one steps back but also many steps back. In this paper, a simplest CAM is adopted in which the state of cell depends on last two steps, i.e. In order to ensure reversibility of CAM, a special method to construct CA's rule must be introduced. The details of analysis of CAM and how to select a reversible rule as follows:

The forward iteration is described as follows; in which f is transition rule _F

$$\begin{aligned} c_i^{j+1} &= f(c_{i-r}^j, c_{i-r+1}^j \ldots\ldots, c_i^{j-1}, c_{i+1}^j \ldots c_{i+r}^j) \quad 1) \\ &= \{ f(c_{i-r}^j, c_{i-r+1}^j \ldots\ldots, 0, c_{i+1}^j \ldots c_{i+r}^j) \text{ while } c_i^{j-1}=0 \\ &= \{ f(c_{i-r}^j, c_{i-r+1}^j \ldots\ldots, 1, c_{i+1}^j \ldots c_{i+r}^j) \text{ while } c_i^{j-1}=1 \end{aligned}$$

In backward iteration c_{i+1}^j. will be treated as the preceding state c_i^j, of the iteration described as follow inwhich g is transition rule:

$$\begin{aligned} c_i^{j-1} &= g(\ c_{i-r}^j, c_{i-r+1}^j \ldots\ldots, c_i^{j+1}, c_{i+1}^j \ldots c_{i+r}^j) \\ &= \{ g(\ c_{i-r}^j, c_{i-r+1}^j \ldots\ldots, c_i^{j+1}, c_{i+1}^j \ldots c_{i+r}^j) \text{ while } c_i^{j+1}=0 \\ &= \{ g(\ c_{i-r}^j, c_{i-r+1}^j \ldots\ldots, c_i^{j+1}, c_{i+1}^j \ldots c_{i+r}^j) \text{ while } c_i^{j+1}=1 \end{aligned}$$

One Dimensional CA rules for 2D CA: The two-dimensional reversible rule is with Wolfram's one-dimensional reversible rules. The number of these rules is 65280 and they are built as follows:

First, we choose two rules of Wolfram's reversible rules such as f1 and f2. Then rule f1 is applied to the rows of a two-dimensional CA and then rule f2 is applied to the columns of the result two-dimension CA. For example, assume the two-dimensional CA as Fig. 2. At the beginning we convert the two-dimensional CA to a

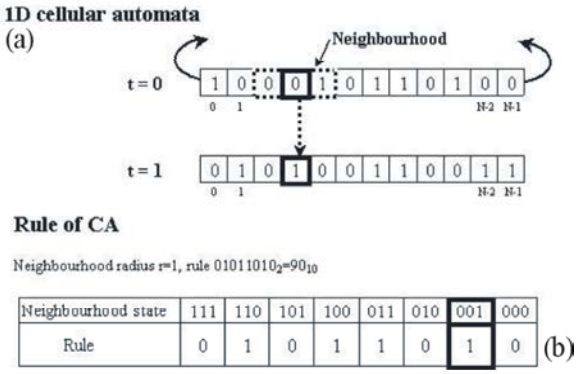

Fig. 1: 1D Cellular automata: (a) Initial configuration and first time step,(b) an example of transition function - CA rule with neighbourhood radius r=1.

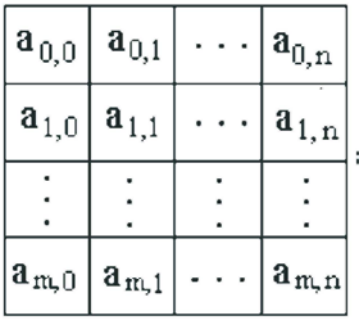

Fig. 2: Two-dimensional CA.

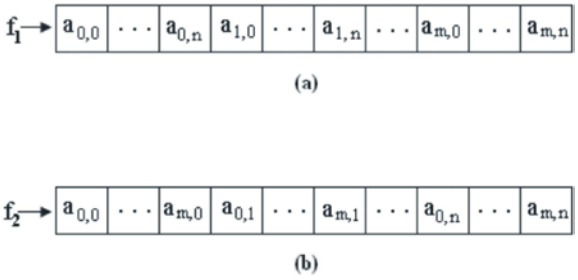

Fig. 3: a) Converting the two-dimensional CA to a one dimensional with re-arranging its rows. b) Converting the two dimensional CA to a one-dimensional CA with re-arranging its columns.

one-dimensional CA with re-arranging its rows in serial (Fig. 3-a). Then we apply the reversible rule f1 to it. Next, the new two dimensional CA configuration once again, is converted to another one-dimensional CA. But this time, the one dimensional CA is obtained through re-arranging the columns of the new configuration matrix of the two dimensional CA in serial, as Fig. 3-b. Then we apply the reversible rule f2 to it. Therefore, a compound two dimensional reversible rule can be considered to be applied once to the CA.

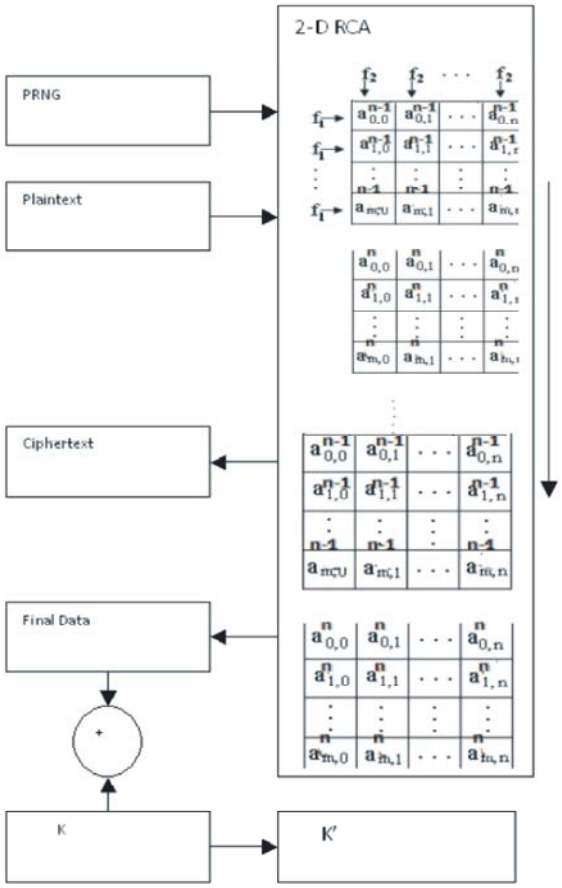

Fig. 4: Encryption using 2-D RCA

Using Two Dimensional Reversible Cellular Automata in Block Cipher: When using two dimensional reversible cellular automata described in the previous section, plaintext is encoded as part of initial configuration C_0 of a CA. Configuration *C*-1 *is* set up with some random data. *C*-1, *C*0 forms initial configuration of CA. Encryption is done by forward iteration of 2-D RCA by fixed number of steps (n iterations) according to some reversible rules f1 and f2 on rows and columns of 2-D RCA. The encryption process is shown in Fig. 4.

Configuration Cn-1 *is* a cipher text. The rule used during encryption is secret key of that transformation. There are two options on how to treat configuration *C*n (called final data) generated by the encryption process. The most secure one assumes that this information is kept secret, which means that configuration *C*n becomes a part of the key. The disadvantage of this option is that the key change with each encryption. In the second option the final data *Cn* is encrypted by applying logical bitwise operation XOR on the final configuration *C* n and selected bits of the key.

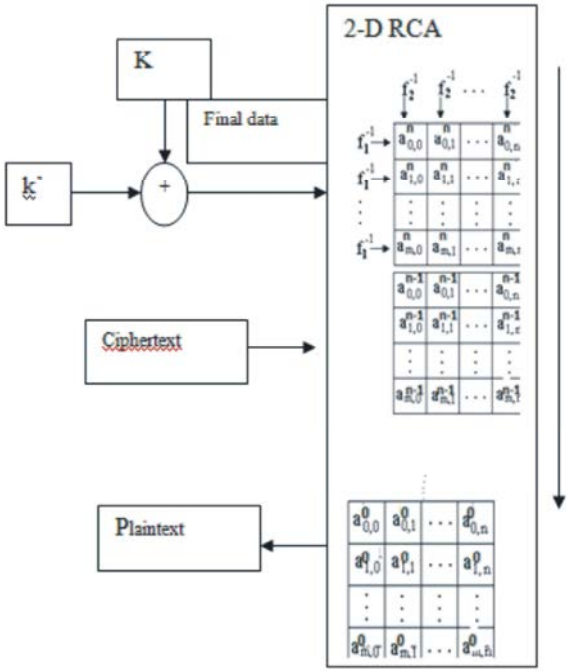

Fig. 5: Decryption using 2-D RCA

Decryption is simply a backward iteration of 2-D RCA with initial configuration composed of final data, ciphertext. The same rule and number of iteration are used as in encryption. Decryption process is shown on Fig. 5.

CONCLUSION

The proposed block encryption algorithm using 2D RCA would definitely overcome the brute force attack & chosen cipher text attack since 2D RCA generates large possible combinations of keys which very difficult to crack down. The rules that are used in the proposed algorithm for the 2D RCA are efficient for cryptic systems since its satisfies some of the important cryptographic properties (avalanche and strict avalanche).

REFERENCES

1. Jonathan Katz and Yehuda Lindell, 2007. Introduction to modem cryptography: principles and protocols, Chapman & Hall/CRC Cryptography and Network Security Series.
2. Blackburn, S., S. Merphy and K. Paterson, 1997. Comments on 'Theory and Applications of Cellular Automata in Cryptography, IEEE Trans Computers, 46(5): 637-638.
3. Biham, E. and A. Shamir, 1991. Differential Cryptanalysis of DES-Like Cryptosystems, J. Cryptology, 4(1): 3-72.
4. Creutz, M., 1986. Deterministic Ising Dynamics," Annals of Physics, 167(62).
5. Wolfram, S., 1985. Cryptography with cellular automata [J] Advances in Cryptology, pp: 429-432.
6. Gutowitz, H., XXXX. Cryptography with Dynamical Systems, manuscript,http www.santafe.edu/ ~hag/ crypto/ crypto.htm
7. Kari, J., 1992. Cryptosystems based on reversible cellular automata, personal communication.
8. Ilachinski, XXXX. Cellular Automata—A discrete universe, World scientific.