Journal of University of Thi-Qar No.1 Vol.3 Sep./2007

Stream cipher using two dimensional Cellular Automata

م.م حيدر إبراهيم هندي /جامعة ذي قار/كلية العلوم

م.م حمدان لطيف جميل/جامعة ذي قار/كلية العلوم

م.م شاكر كاظم علي/جامعة ذي قار/كلية العلوم

thiqaruni.org

الخلاصة:

تم استخدام ماكنة خلوية ثنائية البعد وذلك لاجل التغلب على محدودية القيم المولدة في مولدات السلاسل العشوائية*(pseudo–random generators)* التي تستخدم مسجلات الإزاحة الخطية المرتدة *(linear Feedback shift register)*.وقد تميزت السلاسل الثنائية شبة العشوائية المتولدة بنجاحها في الاختبارات العشوائية *(random tests)* المصممة لهذا الغرض.

Abstract:

The pseudo-random early in cryptography systems, the important of cellular automata has properties which are considered a state machine, high periods.
two–dimensional cellular automata was used to avoid the limitation of the generated periods in the pseudo-random binary sequences such that used in linear shift Feedback registers (LFSR) , the binary sequences that are generated form CA generator are characterized by their success in random tests.

1.Introduction:=

The cellular automata (CA) have been used since the forties of last century. it was used in many physical applications .These applications extended to other fields as biological models, image processing, language recognition, simulation ,computer architecture, cryptography and many other fields.

The Cellular Automata is one of the modern methods used to generate binary pseudo–random a sequences, using registers.

The concept of CA was initiated in the early 1940's by J. Von Neumann and Stan Ulam . Von Neumann showed that a cellular automaton can be universal. He devised a CA, each cell of which has a state space of 29 states, and showed that the devised CA can execute any computable operation. However, due to its complexity, Von Neumann rules were never implemented on a computer. Von Neumann's research pointed to a dichotomy in CA research. On one hand, it was proven that a decentralized machine can be designed to simulate any arbitrary function. On the other hand, the machine (CA) becomes as complex as the function it tries to simulate. This very theoretical dichotomy has since driven research on CA [1].

Based on the theoretical concept of universality, researchers have tried to develop simpler and more practical architectures of CA which can be used to model widely divergent application areas. In this respect, two notable developments can be credited to Conway and Wolfram. In the 1970, the mathematician John Conway proposed his now famous game of life [1] which received widespread interest among researchers. In the beginning of the eighties, Stephen Wolfram has studied in much detail a family of simple one-dimensional cellular automata rules (now famous Wolfram rules) and showed that even these simplest rules are capable of emulating complex behavior. [1]

This type of CA is the One, which is used, now in very wide range of applications. The important issue in CA modeling is to capture the essential features of given phenomena and translate it to a suitable from to attain affecting computations. CA applies useful models for many investigations in natural science. Combinatorial mathematics of computes science. Also they present a natural way to study the evolution of large physical systems and provide a general paradigm for parallel computation, that can be used to efficiently implement a programaning environment, allowing easier access parallel machine facilities and at the same time , hiding many of complexities of under lining parallel architecture .[2]

In this approach will study the type of cellular automata and definition cellular automata and important building block of cellular automata and properties of CA and complexity of CA, implementation proposed two dimensional CA and conclusion

2.Cellular automata:

CA is a framework of fully discrete universe made of cells. Each cell is characterized by an internal state which typical consists of finite number of bits.

A Cellular Automata consist of one array(one dimensional or two) of cells of which can be one of finite number of possible states, updated synchronously in discrete time steps, according to local, identical interaction rule.

The state of cell at the next time step is determined by the current state of surrounding neighborhood of cells.[3]

3.Types of Cellular Automata

Since its inception, different structural variations of CA have been proposed to ease the design and behavioral analysis of the CA as well as make it versatile for modeling purposes. The CA structure introduced by Von Neumann uses 29 states per cell. introduced a machine with 8 states per cell. Arbib provided a simple description of self-reproducing CA in .whereas Banks worked with a CA having 4 states per cell [4].

All these two-dimensional CA are assumed to have a five-cell neighborhood (self and four orthogonal neighbors). The nine-cell neighborhood CA, with two states per cell and appropriate rules, has been shown to be capable of universal computation . This structure has been utilized with a specified set of local rules to create the game of life. The two variations of neighborhood configurations (five and nine) are termed as Von Neumann and Moore neighborhood, respectively. There are extended generalizations of these two neighborhoods configurations - the Rradial and R-axial neighborhoods respectively]. (For both Von Neumann and Moore neighborhood, R = 1.)

Because of its inherent simplicity, the one-dimensional CA with two states per cell became the most studied variant of CA [5]. The neighborhood generally varies from three to five or seven cells .

In another type of CA, the states are assumed to be a string of elements in a Galois field GF(q), where q is the number of states of a CA cell . Additive and linear CA gained popularity in the V LSI era, due to local interaction of simple cells, each having two states `0' or `1' - the elements of the field GF(2). The next state logic of linear and additive CA is expressed in terms of xor and xnor logic gates.

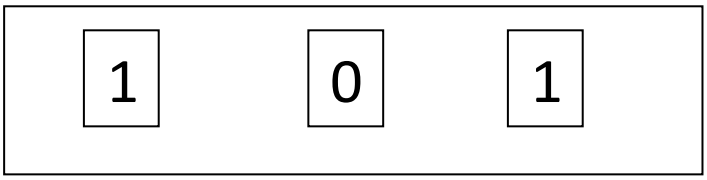
Recently, Paul has introduced the theory of GF(2^p) cellular automata over Galois extension field GF(2^p)A cell of the GF(2^p) CA consists of p memory elements and can store an element of GF(2^p). The GF(2^p) CA provides the required structure for hierarchical modeling of different physical systems [6]. For example, with the same CA configuration, a circuit can be analyzed from the gate level as well as the transistor level. Cellular automata on multi-dimensional grids have also been proposed . The grids have either null or periodic boundary. In null boundary configurations the boundary cells are assumed to have `null' (logic `0') dependency. A variation of the null boundary configuration is the fixed boundary configuration in which the boundary cells instead of being considered `0' are replaced by a fixed value A periodic boundary is one in which the grid is considered to be folded That is, for one dimension, the right most cell is the neighbor of the left most one and vice versa. The concept of intermediate boundary CA has been proposed in which an intermediate cell acts as the right(left) neighbor of the rightmost (leftmost) cell of the grid. Intermediate boundary CA are found to generate better pseudo-random patterns [7].

4 Building the Cellular Automata

4.1 The Cell

The basic element of CA is the cell. A cell is kind of memory element and stores to say it with easy words (states).

In the simplest case, each cell can have the binary states 0 or 1. In more complex simulation the cells can have more different states, (It is even thinkable, that each cell can have more two or more states) as how fig|(1).[8]

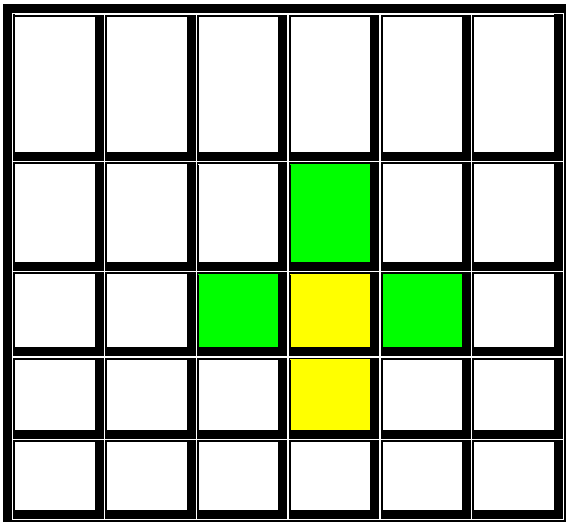


Fig(1) cell state

4.2 The Lattice

These cells are arranged in special web a lattice . The simplest one is the one-dimensional lattice mean that all cell are arranged in a line like string such fig(2). The most common CA are built in one or two dimension. consider the two dimensional Cain fig(3)[9]

Fig(2)One dimensional Cellular Automata



Fig(3) Two dimensional Cellular Automata

4.3 Neighborhoods

These cells are arranged in lattice, which represents a static state. that introduce dynamics into the system. We have to add rules, the rule depends on the size and the type of the spatial region in which a cell needs to update its value this region is called neighborhood. In principle there is restriction on the size of the Neighborhood. It's the same for all cells. However in practice .Its often made up of adjacent cells only. If the neighborhood is too large, the complexity of the rule may be unacceptable (complexity usually grows exponentially fast with the number of cells and states in the neighborhood [10].

The one dimensional cellular automata neighborhood three such that fig(2)(the center is original cell and two right and left cells)

Fig(4)the two dimensional neighborhoods

Fig(4) illustrate Neighborhood structures considered for two-dimensional cellular automata. In the cellular automaton evolution, the value of the center cell is updated according to a rule that depends on the values of the shaded cells. Cellular automata with neighborhood (a) are termed ``five-neighbor square''; those with neighborhood (b) are termed ``nine-neighbor square.'' (These neighborhoods are sometimes referred to as the von Neumann and Moore neighborhoods, respectively.) Totalistic cellular automaton rules take the value of the center site to depend only on the sum of the values of the sites in the neighborhood. With outer totalistic rules, sites are updated according to their previous values, and the sum of the values of the other sites in the neighborhood. Triangular and hexagonal lattices are also possible, but are not used in the examples given here. Notice that five-neighbor square, triangular, and hexagonal cellular automaton rules may all be considered as special cases of general nine-neighbor square rules.[11].

4.4 Cellular Automata Rule

The rule of CA can functions that have a balanced truth table, a balanced rule .For example XOR is balanced rule, because it has balanced output result for all of it s input possibilities, while (and) it has not (OR) is balanced rule and cellular automata is discrete universe made of cells containing large numbers of simple of identical components, with local interactions. They consist of lattice of sites, each with a finite set of possible values, the values of the site evolve synchronously in discrete time steps according to identical rules. The rule of a particular site is determined by the previous value of neighborhood of sites around it. [3]

The one – dimensional cellular automata consists of a (possibly infinite) line of with values (where, S_i is the next value dependent r of cell is rule and these (S_{i-r} , S_{i-r+1} ,……., S_{I+r}) are the cells which include the rules) . [8]

The simple one – dimensional cellular automata consists of a circular register with N cells ,each have a value (a_i) equal to (0 or 1) .
The value are updated synchronously in discrete time steps according to the rule

$$a_i^{(t+1)} = a_{i-1}^{(t)} \ \text{XOR} (a_i^{(t)} \ \text{OR} \ a_{i+1}^{(t)}) \quad \text{.....(1)}$$

or , equivalently

$$a_i^{(t+1)} = (a_{i-1}^{(t)} + a_i^{(t)}) + a_i^{(t)} + a_{i+1}^{(t)} + a_i^{(t)}) \bmod 2 \quad \text{.....(2)}$$

There are several possible lattices and neighborhood structures for two-dimensional cellular automata. This paper considers primarily square lattices, with the two neighborhood structures illustrated in Fig. 4. A five-neighbor square cellular automaton then evolves in analogy with Eq. (3,4) according to

$$a_{i,j}^{(t+1)} = \phi[a_{i,j}^{(t)}, a_{i,j+1}^{(t)}, a_{i+1,j}^{(t)}, a_{i,j-1}^{(t)}, a_{i-1,j}^{(t)}] \text{.....(3)}$$

Here we often consider the special class of totalistic rules, in which the value of a site depends only on the sum of the values in the neighborhood:[11]

$$a_{i,j}^{(t+1)} = f[a_{i,j}^{(t)}, a_{i,j+1}^{(t)}, a_{i+1,j}^{(t)}, a_{i,j-1}^{(t)}, a_{i-1,j}^{(t)}] \text{.....(4)}$$

And the function F is dependent the lattice of neighborhood

4.5 The Initial State

The initial state of the register is used as seed or key .the values a(t) attained a particular cell through time can then serve as a random sequence .[10]

In one dimensional cellular automata most important concepts is to feed our cellular with balanced initialization by using a balanced rule to produce a balance output [4] . the anther important of cellular automata can using zero Initial value the different of LFSR the can using zero Initial value. [10].

The two dimensional cellular automata initial value most not all zero and using more one states of cell such that byte or two byte (character or integer).

1.5. Cellular Automata Properties: -
2.parallelism : -
parallelism means the updating of an individual cell is performed independently of each other.

2. Locality:-

The future state of each cell depends only on the current state of the cell and the states of the cells in the neighborhood .

3.Homogeneity :-
Means that each cell is update according to the same rule .

4.A Cellular Automata is a discrete simulation method. Hence space and time are defined in discrete steps

6. Cellular Automata Complexity:

the most common used are one –dimensional lattice of N stage.

The complexity =2^n where used binary state (0,1) if the input is an alphabetic characters (a,b,c,…….,z) then the complexity=26^n.the complexity of cellular automata with non-linear (if we use XOR)or non-linear (if we use AND).

the complexity of cellular automata with linear rule and will increase ,where the number of neighbors cells is increase around of center cell.[12]

in two dimensional cellular automata for lattice [n,n] the complexity = $2^{n\times n}$ where used binary state alphabetic character complexity =$26^{n\times n}$

7. CA Applications

cellular automata in a large number of application domains. CA have been used to model biological systems from the level of intracellular activity to the levels of clusters of cells, and population of organisms. CA have been used to model the kinetics of molecular systems and crystal growth in chemistry. In physics, the applications cover the study of dynamical systems starting from the interaction of particles to the clustering of galaxies.

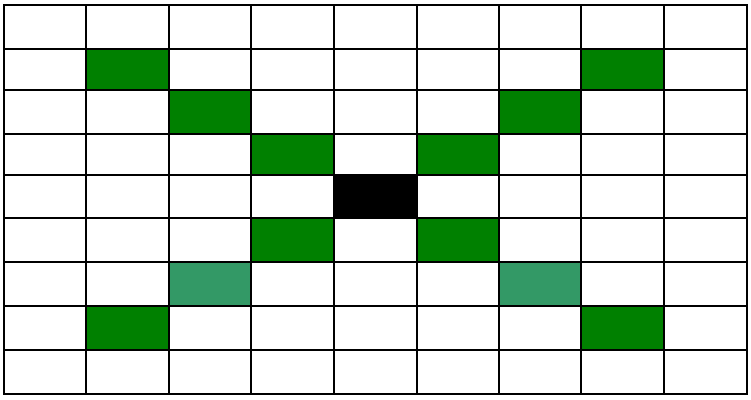
In the field of computer science, cellular automata based methods have been employed to model the Von Neumann (self-reproducing) machines as well as the parallel processing architecture. Beyond the domain of natural science, CA have also been used to study other diverse fields [1].

In view of such diversity, we are presenting the main applications that have not only taken the research on cellular automata to new heights, but also made researchers from different fields join and collectively exploit the exciting world of cellular automata. [1]

8. Implementation:-

In this approach implemented two dimensional cellular automata (2D-CA) cryptosystem using C++ language because effective to processing the data and easy processing the character and integer that used in cryptography.

The proposed method of 2D-CA neighborhood has 13 cells (12 neighbors and one original cell) and similar "X" letters that show in Fig (5).



Fig(5)the proposed method neighborhood

The proposed method has variable cell state because using variable prime

Number (p) that input in executive program and cell state is equal $\log_2(p)$

And that cell state will increase the security of the method because increasing

The complexity of encryption..

The size of 2D-CA dependent variable number (s) then 2D-CA size equal A[s,s].

The rule of encryption after input the initial will update cellular automata dependent of neighborhood by using equation (5)

....(5) $$a_{i,j} = [a_{i,j} + \sum_{k01}^{3} (a_{i-k,j-k} + a_{i-k,j+k} + a_{i+k,j+k} + a_{i+k,j-k})] \bmod p$$

Such that

$$0 \le \mathrm{i}+\mathrm{k}\,,\,\mathrm{j}+\mathrm{k} < \mathrm{p}$$
$$0 \le \mathrm{i}-\mathrm{k},\,\mathrm{j}-\mathrm{k} < \mathrm{p}$$

After update the CA then using all element in encryption by using two equations linear encryption such that eq (6)

$$\text{.....(6)}\; C_{s*s*l+i*s+j} = (A^{l}{}_{i,j} + M_{s*s*l+i*s+j}) \bmod p$$

And nonlinear such that eq(7).

$$\text{....(7)}\; C_{s*s*l+i*s+j} = (A^{l}{}_{i,j} * M_{s*s*l+i*s+j}) \bmod p$$

Which

L is number of update CA

S is size of CA

P is prime number

M is plaintext that given from file "message.txt"

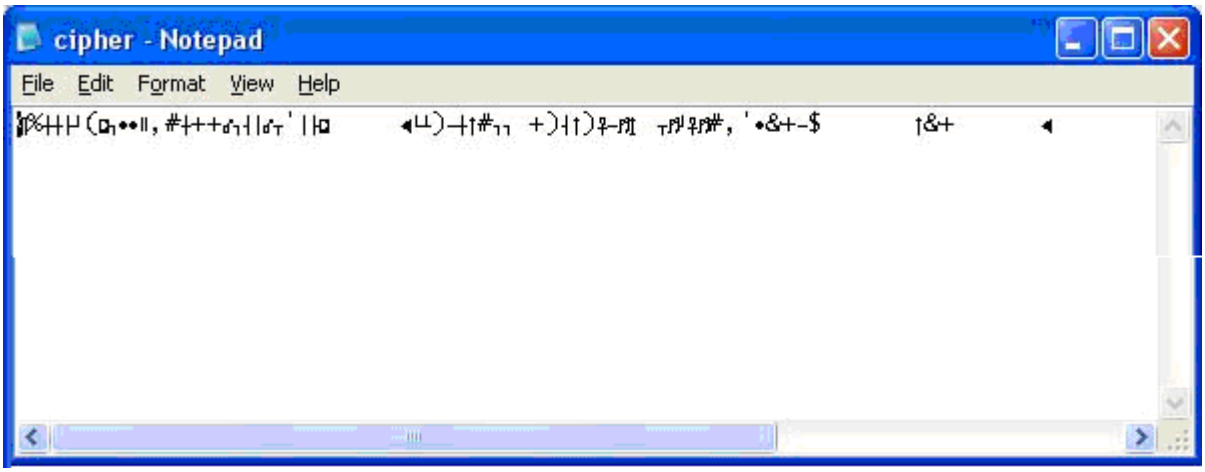
C is ciphertext put on file"cipher.txt" such that show Fig(7).

In decryption that using similar rule of update the CA and calculated $a_{i,j}$

For nonlinear decryption calculated the inverse of the element by equation (9)

$$a_{i,j}^{-1} = (a_{i,j}^{l})^{p-1} \bmod p \forall i, j \quad \text{.....(9)}$$

And calculated the plaintext by using equation (10)



Fig(7)the cipher file interface

.....(10) $$M_{s*s*l+i*s+j} = (A^{-1}{}_{i,j} + C_{s*s*l+i*s+j}) \bmod p$$

.....(11). $$M_{s*s*l+i*s+j} = (A^{-1}{}_{i,j} * C_{s*s*l+i*s+j}) \bmod p$$

Which

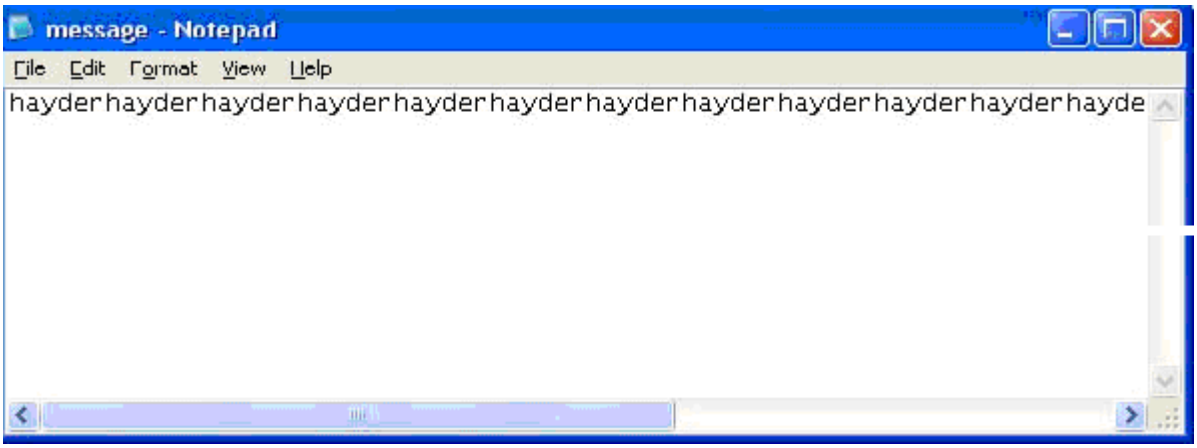
L is number of update CA

S is size of CA

P is prime number

M is plaintext that on the file "message.txt" such that show Fig(8).

C is cipher text that on file"cipher.txt"



Fig(8) the message file

The important of the proposed method is high complexity that calculated by Goasas field G(p)

9.Conclusion

In this approach detailed of various model application of cellular automata also provide different theoretical development of cellular automata field .

The cellular automata dynamic machine using discrete time and space ,have high periods case useful than LFSR .

The two dimensional cellular automata is more effective than one dimensional because using more two cell neighborhood and the lattice of neighborhood .

The proposed method is effiency than traditional two dimensional cellular automata because the number cells of neighborhood and ship of neighborhood that similar 'X' letter which have high complexity and is not effect to speed .

The proposed method using more 2byte the cell state and using nonlinear (discrete logarithm problem DLP) that provided high security

Reference:-

[1]niloy ganguly, sikdar "a survey on cellular automata " Dresden university of technology ,germany 2003.

[2]Curis f.gerald & patrick o.wheatley,"{applied numerical analysis",addisn wisely publishing company,(1984).

[3]David .j . Eck "one dimensional cellular automata ',internet

http://www.david.com(1994)

[4] E. R. Banks. Information Processing and Transmission in Cellular Automata. PhD thesis, M. I. T., 1971.

[5] S. Wolfram. Statistical Mechanics of Cellular Automata. Rev. Mod. Phys., 55(3):601{644, July 1983.

[6] K. Paul. Theory and Application of GF(2p) Cellular Automata. PhD thesis, B. E. College, (Deemed University),Howrah, India, 2002.

[7] P. Pal Chaudhuri, D. R. Chowdhury, S. Nandi, and S. Chatterjee. Additive Cellular Automata { Theory and Applications,volume 1. IEEE Computer Society Press, CA, USA, ISBN 0-8186-7717-1, 1997.

[8] Giovanni adorni ,Federico bergenti and Stefano cagnoni " cellular automata approach to pattern classification" (1998).

[9]akeel n. mahmoud,"apseudo-random number generator using cellular machine.(2000).

[10]:David j.eck ,"the neighborhood", internet

, http://www.david.com(1994)

[11]Stephen wolfram ,"cryptography with cellular automata", internet ,http:\\www.stephen wolfram.com.

[12]Bruce schneier,"applied cryptography", john wiley&son,(1996).