Research of Encryption Based on Chaotic Cellular Automata

S.L. Liang
School of Physics
Northeast Normal University, 130024
Changchun, China

S. Gong
School of Physics
Northeast Normal University, 130024
Changchun, China

D.F. Wang
School of Physics
Northeast Normal University, 130024
Changchun, China

X.B. Zhao
School of Physics
Northeast Normal University, 130024
Changchun, China

G.Y. Li
School of Physics
Northeast Normal University, 130024
Changchun, China

***Abstract*-In this paper we proposed a block cryptosystem based on 1d-k5 Chain C CA, by alternatively iterating left- and right-toggle chain rules, this kind of encryption is achieved by backward iteration and decryption is realized via forward iteration. From theory proof, we can ensure the security of the cryptosystem, and make mostly confusion and diffusion function. Experimant shows that this cryptosystem has a large key space and good scrambling effect and can resist brute attack and differential attack effectively.**

Keywords-cellular automata (CA); Chaos, encryption; cryptanalysis

I. INTRODUCTION

Cellular automata(CA) are dynamical systems in which space and time are discrete. A Cellular automata consists of an array of cells, each of which can be in one of a finite number of possible states update synchronously in discrete time steps, according to local identical interaction rule.CA have been used as encrypting ways in the past.

Wolfram[1] first introduced the one-dimensional (1-D) Rule 30 CA as a pseudorandom number generator; additive extended CA were used for generating pseudorandom sequences in [2] and [9]; Chowdhury[3] extended the theory of 1-D CA and proposed an M x N two dimensional (2-D) restricted vertical neighborhood (RVN) CA with a maximum length of 2^(log2m)(2^n-1); Cattell [4] constructed a (2^2n-1) long 2 X N hybrid CA with regular configuration, and demonstrated that 2-D CA performs, on average, better than 1-D linear hybrid CA. By nature, CAs are dynamic systems in which space and time are discrete and consist of limited states and the quality of the random numbers generated by CAs has not been well established. CAs used as random number generators (RNGs) are efficient but are far from ideal as RNGs for generating encryption keys.

In CA-based encryption studies, Guan[5] and Kari[6] designed a CA-based public-key cryptosystem in which encryption is performed by iterating the CA in the forward direction and decryption is achieved by iterating CA backward. Habutsu used an irreversible dynamic system to obtain ciphertext by the iteration of an inverse chaotic map from an initial point, which denotes a plaintext, and to decrypt via forward iteration. Gutowitz [8]pointed out that dynamics systems without predecessor cannot always be iterated backward thus such systems are not suitable for block cipher applications. Gutowitz[11] defined a “toggle” rule, and all toggle rules are irreversible. Using irreversible rules several ciphertexts can be generated for one plaintext via backward iteration. Without the knowledge of link information, this greatly increases the difficulty of finding the plaintext from multiple ciphertexts; during decryption, ciphertext can be uniquely determined with the deterministic system and its initial state. The Gutowitz’s system has obvious shortcomings: when the toggle rules are used as the secret keys for cryptographic systems, the system fails to consider selecting proper rules. This inevitably results in the use of non-chaotic rules. Such rules and models based on them have fetal problem of short periodicity, and this is equivalent to using weak keys in cryptography. Cryptanalytic attack using known ciphertext thus becomes easier. To overcome the shortcomings of the cryptosystem proposed by Gutowitz[7], we adopted chain rules to generate encryption keys. Similar to Data Encryption Standard (DES), this method uses chaotic CA to construct encryption algorithm with an S-box function. With the chaotic chain rules, encryption is realized by running the CA backward, and decryption is done by running the CA forward. Our method to some extend solves the difficult problem in cryptography

that cryptographic systems are required to be non-linear and irreversible. In addition, the chaotic nature in chain rules can help achieve maximally chaotic and diffusive effects.

II. Design of Encryption Algorithms

Wuensche directly describes the properties of CA dynamic systems using reverse algorithms to back iterate CA "basins of attraction"[10]. He points out that the chaotic CAs have lower convergent rate which is reflected by the fact that the number of basins of attraction barely increases with increasing number of systems, indicating that the increases states are all distributed on a single transient tree without branches and that the period of basin of attraction becomes longer. Wuensche defined a class of chain rules which are maximally chaotic CA rules. These chain rules have toggle property and have only one predecessor, and all the predecessors form a 'chain', indicating the period of states become longer. We use a 1-D five neighborhood chain rule CA. The status of five cells at time t is denoted by a^t_i-2, …. A^t_i+2, during forward iteration, the next state a^(t+1)_i of a^(t)_i can be described by the following:

$$a_i^{t+1} = \tau\ (a_{i-2}^t, a_{i-1}^t, a_i^t, a_{i+1}^t, a_{i+2}^t) \quad (1)$$

For a chain rule with left-toggle property, changing the value of the leftmost cell of thearray results in the inverse of the original value, which can be described by the following formula:

$$1 - a_i^{t+1} = \tau\ (1 - a_{i-2}^t, a_{i-1}^t, a_i^t\ a_{i+1}^t, a_{i+2}^t) \quad (2)$$

For a CA with only '0' and '1' two statuses and both (1) and (2) are satisfied, its reverse iteration can be expressed by the following:

$$a_{i-2}^t = \tau\ (a_i^{t+1}, a_{i-1}^t, a_i^t, a_{i+1}^t, a_{i+2}^t) \quad (3)$$

Proof:

If a CA has 0 and 1 two statuses only, there are only two relationships between a^(t+1)_i and a^(t)_(i-2):

1. When a^(t)_(i-2) = a^(t+1)_i, formula (3) can be obtained from (1);

2. When a^(t)_(i-2) ≠ a^(t+1)_i, now a^(t)_(i-2) = 1- a^(t+1)_i and a^(t+1)_(i) = 1- a^(t)_(i-2), thus formula (3) can be obtained from (2). Proof completed.

From formula (3), if the statuses of a^t(i-1), a^t(i), a^t(i+1), a^t(i+2) at time t and status of a^(t+1)_(i) at time t+1 are known, the status of a^t(i-2) at time t can be uniquely determined. This proves that this class of CA can be reversely back iterated.

TABLE I. Chaotic Chain Rules ecb5134a (ZL=0.625;ZR=1) Forward iteration.

Iteration	Forward iteration (binary)	Boundary condition
0	10101010101010101010101010101010	1000
1	00110110010011011001011011001	0111
2	00000100000010010000000010010000	1000
3	11100011100100000000011110011	0111
4	11100101101101000111000010001	1000
5	01000001001001110111001101000	0111
6	01000110101001010111000001110	1000
7	10001010101001101111001111110	0111
8	10010011011011011111000010110	1000
9	00011111011000001011010011001	0111
10	00101111011010000010011111000	

TABLE II. Chaotic Chain Rules ecb5134a (ZL=0.625;ZR=1) Backward iteration.

Iteration	Back iteration (binary)	Boundary condition
0	00101111011010000010011111000	0111
1	00011111011000001011010011001	1000
2	10010011011011011111000010110	0111
3	10001010101001101111001111110	1000
4	01000110101001010111000001110	0111
5	01000001001001110111001101000	1000
6	11100101101101000111000010001	0111
7	11100011100100000000011110011	1000
8	00000100000010010000000010010000	0111
9	00110110010011011001011011001	1000
10	10101010101010101010101010101010	

The current algorithm is an iterative block cipher algorithm with 128-bit block and 128-bit symmetric keys; a 1-D 5-neighborhood chaotic chain rule, similar to DES' non-linear cryptographic function, is used to encrypt plaintext by backward iteration of the chain rules and to decrypt ciphertext via forward iteration. Diffusion and confusion are achieved by iterating chain rules CA alternatively with left- and right-toggle properties for a total of 16 times. The key space and plaintext space are both 2^128, which is large enough to resist brute-force attack.

III. Experimental analysis

Diffusion analysis

The diffusion and confusion functions are achieved by alternatively iterating 16 times the left- and right-toggle chain rules CA. We analyze the error propagation of ciphertext by plaintext with a fixed key and the error propagation by key with fixed plaintext:

A. Error propagation with a fixed key

We set all 128 bits to zero, change any one of them (from 0 to 1), and finally, compare the differences between altered ciphertext and the original one. The figure below shows the errors between the input plaintext and output ciphertext.

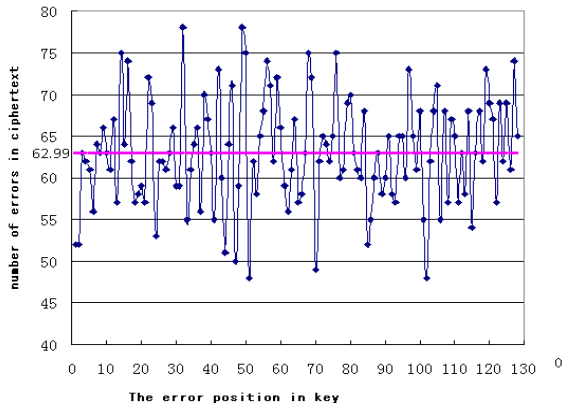

FIGURE I. NUMBER OF ERRORS IN CIPHERTEXT VS. ERROR POSITION IN PLAINTEXT.

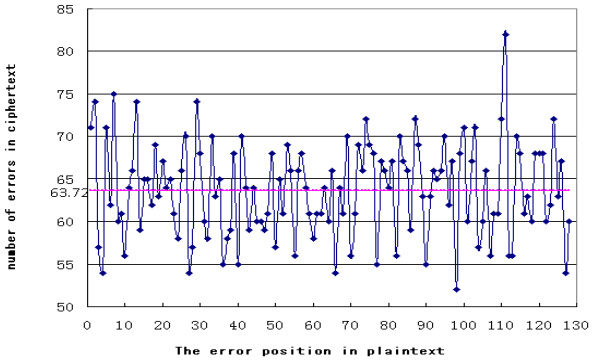

FIGURE II. NUMBER OF ERRORS IN CIPHERTEXT VS. ERROR POSITION IN KEY

The figure1 above shows that the changed bits in the plaintext correspond to the number of differences. For example, the change from 0 to 1 of the 111st bit in plaintext results in a change of maximum 82 bits in its corresponding ciphertext; change of the 98th bit results in the change of minimum 52 bits; on average, errors are 63.72 if any of 128 bits is changed. The average number of about half of 128 indicates that the proposed scheme has fairly good diffusion property with a fixed key.

B. Error propagation with fixed plaintext

The error propagation of ciphertext with fixed plaintext refers to the effect of change of any bit of the key. We set all 128-bit plaintext to 1 and the key to 128-bit 0.

From the figure 2 above, we learn that the number of errors in the ciphertext is 48 if the 51st bit of the key changes from 0 to 1; similarly the change of 32nd bit in the key results in a total of 78 bits change in the ciphertext. On average, a change of single bit in the key causes a change of about 63 bits in the ciphertext, and this number indicates good diffusion property.

C. Differential cryptanalysis

The proposed scheme has 2^127 fixed differential values for a set of 128-bit plaintext (without considering the situation of bit 128 is zero). For each fixed differential value, there are corresponding 2^128 output values. Therefore, the computation for the differential values of a plaintext is 2^128, and the total computation for all 128-bit plaintext is 128 X 2^128 = 2^135.

D. Image encryption

FIGURE III. SOURCE LINA IMAGE

FIGURE IV. ENCRYPTED LINA IMAGE

The proposed cryptosystem can be applied to any type of digital data. Computer simulations demonstrated that the encrypted data can be recovered completely bit-by-bit. Figures 3 and Figures 4 are source image and encrypted image. The decrypted image exactly matches the original one.

IV. SUMMARY

In this method, we use chaotic CA to construct a block cryptosystem. Encryption is achieved by backward iteration and decryption is realized via forward iteration. Experimental Analysis shows that diffusion and confusion properties are maximally achieved while strong encryption is maintained. In addition, the proposed scheme can best resist differential attacks and exhaustive plaintext and key searches.

ACKNOWLEDGEMENTS

This work was supported by Natural Science Foundation of China (Grant No. 61370228).

REFERENCES

[1] S. wolfram, Cryptography with Cellular Automata, proceedings os Crypto'85, pp. 429-432,1985.

[2] Marco Tomassini, Moshe Sipper, Mathieu Perrenoud. On the Generation of High-Quality Random Numbers by Two-Dimensional Cellular Automata.[J] .IEEE trans.Compu., 49(10):1146-1151,2000.

[3] Chowdhury D Roy, Subbaro P. Chracterization of Two-Diminsional Cellular Automata Using Matrix Algebra, [J] .Information Sciences, 71:289-314,1993.

[4] Kevin Cattell, Zhang Shujian, Micaela Serra, et al.2-by-n Hybrid Cellular Automata with Regular Configuration: Theory and Application. [J]. .IEEE trans.Compu., 48(3):285-295,1999.

[5] P. Guan, Cellular Automata Public-Key Cryptosystems, Complex Systems Vol.1,1987.

[6] J. Kari, Cryptosystems based on reversible cellular automata University of Turku, Finland preprint.1992.

[7] H.Gutowitz,"Cryptography with dynamical systems" in Cellular Automata and Cooperative Systems, ed. N. Boccara et.al., Kluwer Academic Publishers,pp.237-274, 1993.

[8] Wuensche, A., "Classifying Cellular Automata Automatically; Finding gliders, iltering, and relating space-time patterns, attractor basins, and the Z parameter", COMPLEXITY,Vol.4/no.3, 47-66, 1999.

[9] A.K. Das and P.P. Chaudhuri, "Vector Space Theoretic Analysis of Additive Cellular Automata and Its Applications for Pseudo-Exhaustive Test pattern Generation," IEEE Trans. Computers, Vol.42, pp.340-352,1993.

[10] Wuensche, A., and M.J. Lesser. "The Global Dynamics of Cellular Automata; An Atlas of Basin of Attraction Fields of One-Dimensional Cellular Automata" Santa Fe Institute Studies in the Sciences of Complexity, Addison-Wesley, Reading, MA, 1992.

[11] Complex and Chaotic Dynamics, Basins of Attraction, and Memory in Discrete Networks", ACTA PYSICA POLONICA B, Vol 3, No 2, 463-478, 2010.