Encryption Based on Reversible Cellular Automata+

Zhang Chuanwu, Peng Qicong, Li Yubo*
Institute of Communication and Information Engineering
University of Electronic Science and Technology of China
Chengdu, 610054, China

Abstract: With the development of information technology, information security as well as the implementation of encryption system becomes more and more complexity, and therefore new methods is explored to simplify complexity of the implementation. CA has the characters of simplicity of basic components, locality of CA interactions, massive parallelism of information processing, and exhibits complex global properties, which make it suitable for the application in cryptography. Based on the reversible CA with input boundary, a new method of encryption is presented in this paper, the key of the new method consists of the reversible CA, the vectors input from the input boundary, and the number of the iteration. Evidently, it has larger key space than other methods with only the reversible CA itself as the key.
Keywords: Cellular Automata (CA), Reversible Cellular Automata (RCA), Input Boundary, and Block Cipher.

I. Introduction

With the development of the information technology, information security as well as the implementation of encryption system becomes more and more complexity, therefore new methods is explored to simplify complexity of the implementation. CA is a conception introduced by Ulam and Von Neumann in their study on the self-organized system. Stephen Wolfram was the first to propose a mathematical basis for a class of one-dimensional CA. 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[1,2], which make it suitable for application in cryptography.
In 1985, Stephen Wolfram used iteration of the CA with rule 30 to generate the key stream and used in the stream cipher[3], this is the first time of CA applied in cryptography. S. Nandi presented a block encryption/decryption based on the even permutations of CA [4], but the key space was restricted. P. Guan provided an approach of public crypto-system based on RCA[5], however, it lacks of systematic approach to construct. Based on the RCA with input boundary, a new method of encryption is presented, the key of the new method consists of the RCA, the vectors input from the input boundary, and the number of the iteration. Evidently, it has larger key space than other methods with only the RCA itself as the key.

+ Supported by 30th Institute of the Ministry of Information Industry (2000JS06.1.2ZS0601)
Zhang Chaunwu, Email: firste@sina.com

II. Cellular Automata

CA is dynamic system with discrete state, discrete space and discrete time. It consists of array of cells, each cell can be a state of the state space, and the states of the cells updated according to the states of its neighborhood and itself synchronously.

A CA is a 4-tuple (A,S,f,B)

Where $A=\prod_{i=1}^{d} N_i = N_1 \times N_2 \times \Lambda \times N_d$ is a d-dimensional array and their positions are indexed by $\vec{i}=(i_1,i_2,\Lambda\ ,i_d)$, the set of d-tuples of integers.

S is a finite state set of $Z_k=\{0,1,\Lambda\ k\}$.

f is the local rule of CA presented as a function from the states of neighborhood cells $\{\vec{j}=(j_1,\Lambda\ ,j_d)\,\|\, j_1-i_1\,|\le r_1,\Lambda\ ,|\, j_d-i_d\,|\le r_d\}$ of $\vec{i}=(i_1,i_2,\Lambda\ ,i_d)$ to the state of itself:

$$x_i^{t+1}=f(x_{i+j}^{t}\,\|\, j_1-i_1\,|\le r_1,\Lambda\ ,|\, j_d-i_d\,|\le r_d)$$

0-7803-7547-5/02/$17.00 ©2002 IEEE

(1)

Where $\vec{r} = (r_1, r_2, \Lambda, r_d)$ is the radius vector of f.

B is the boundary conditions of CA, which deals with the situation when the neighborhood $\{\vec{j} = (j_1, \Lambda, j_d) \| j_1 - i_1 | \le r_1, \Lambda, | j_d - i_d | \le r_d\}$ of a cell $\vec{i} = (i_1, i_2, \Lambda, i_d)$ is out of the space $A = \prod_{i=1}^{d} N_i = N_1 \times N_2 \times \Lambda \times N_d$. We always assume null boundary taking the states of the neighborhood out of the space as 0, due to its advantage in the implementation of VLSI.

The local rule f determines the global function F

$$F : (x_i^{t+1} | \vec{i} \in A) = F(x_i^t | \vec{i} \in A) = (f(x_{i+j}^t \| j_1 - i_1 | \le r, \Lambda, | j_d - i_d | \le r) | \vec{i} \in A)$$

Elementary CA[1,6,7,8] is the simplest CA with $d = 1, S = (0,1), r = 1$. A rule is equivalently defined by specifying the value assigned to each of the 2^3 possible 3-tuple $(x_{i-1}^t x_i^t x_{i+1}^t)$ configurations of site values as $\{f_7 = f(111), \Lambda, f_1 = f(001), f_0 = f(000)\}$, so there are $2^{2^3} = 256$ possible rules. A convenient notation assigns a "rule number" $I_f = \sum_{i=0}^{7} f_i 2^i$ to each of the 256 rules of this type[6]. For example, function $x_i^{t+1} = x_{i-1}^t + x_i^t + x_{i+1}^t$ corresponding to the rule number 150 for which $\{f_7 f_6 f_5 f_4 f_3 f_2 f_1 f_0 = 10010110\}$.

III. Encryption Based on the Revertible Cellular Automata with Input Boundary

For the input boundary CA, the sequence of the vectors $\{V^t = (v_0^t, 0, \Lambda, 0, v_{N-1}^t)^T, t = 0,1,2,\Lambda\}$ input from the boundary of CA is taken module 2 addition with the states of CA, and the state transition equation is:

$$X^t = F(X^{t-1}) + V^{t-1} \qquad (2)$$

Where $X^t = (x_0^t, x_1^t, \Lambda, x_{N-1}^t)^T$ is the states or configuration of CA at time t, let X^0 be initial state of CA, iterate (2) n times, we have:

$$X^t = F(\Lambda\ (F(\Lambda\ (F(F(F(X^0) + V^0) + V^1) + \Lambda) + V^i) + \Lambda) + V^{t-1}) \qquad (3)$$

If F is revertible, then the CA is reversible, and the transition equation of the inverse CA can be denoted as:

$$X^{t-1} = F^{-1}(X^t + V^{t-1}) \qquad (4)$$

Iterate (4) n times, we have:

$$X^0 = F^{-1}(\Lambda\ (F^{-1}(\Lambda\ (F^{-1}(F^{-1}(X^t + V^{t-1}) + V^{t-2}) + \Lambda) + V^i) + \Lambda) + V^0) \qquad (5)$$

The forward and backward transition equations (3) and (5) show that: if the CA F, the number of the iteration t, and the input vectors of $\{V^t = (v_0^t, 0, \Lambda, 0, v_{N-1}^t)^T, t = 0,1,2,\Lambda\}$ are determined, we can generate X^0 from X^t, and vice versa. If one of them is absent, X^0 and X^t cannot be determined each other. This property provides an approach to encryption. In order to simplify the analysis, we assume that the CA are linear, thus can use matrix to analyze the transition equation and can analyze the encryption based on RCA with input boundary.

If CA is linear, then F is linear. The transition equation of the CA with input boundary is as follows:

$$\begin{cases} x_0^t = v_0^{t-1} + a_{0,0}x_0^{t-1} + a_{0,1}x_1^{t-1} \\ x_1^t = a_{1,0}x_0^{t-1} + a_{1,1}x_1^{t-1}a_{1,2}x_2^{t-1} \\ \Lambda \\ x_{N-1}^t = a_{N-1,N-2}x_{N-2}^{t-1} + a_{N-1,N-1}x_{N-1}^{t-1} + v_{N-1}^{t-1} \end{cases}$$

It can be rewritten as:

$$X^t = TX^{t-1} + V^{t-1} \qquad (6)$$

Where

$$T = \begin{bmatrix} a_{0,0} & a_{0,1} & 0 & \Lambda & \Lambda \\ a_{1,0} & a_{1,1} & a_{1,2} & 0 & \Lambda \\ O & O & O & O & O \\ \Lambda & 0 & a_{N-2,N-3} & a_{N-2,N-2} & a_{N-2,N-1} \\ \Lambda & \Lambda & 0 & a_{N-1,N-2} & a_{N-1,N-1} \end{bmatrix}$$

T is transition matrix of the CA with null boundary.

Iterate equation (6) n times, we have:

$$X^t = T^t X^0 + \sum_{j=0}^{t-1} T^{t-j-1}V^j \qquad (7)$$

In equation (7), if the transition matrix T is nonsingular, then the state of corresponding CA is injective, thus the CA is reversible. The inverse of the RCA is also a CA[9]. So, if a reversible T is the matrix corresponding to a RCA, then there exist a H corresponding to a CA, which satisfies $H = T^{-1}$. It can be reached that:

$$X^{t-1} = H(X^t + V^{t-1}) = T^{-1}(X^t + V^{t-1}) \qquad (8)$$

Iterate equation (8) t times, we have:

$$X^0 = H^n X^n + \sum_{j=0}^{n-1} H^{j+1}V^j = T^{-n}X^n + \sum_{j=0}^{n-1} T^{-j-1}V^j \qquad (9)$$

Equation (7) and (9) are the state transition equations of a pair of RCA, respectively. And they are encryption and decryption equation of the system. Paper [10] has studied and listed the RCA with m sequence, and thus can be used in our method.

The key of the system consists of the number of RCA, the number of iteration p, and the p input vectors $\{V^t = (v_0^t, 0, \Lambda, 0, v_{N-1}^t)^T, t = 0,1,2,\Lambda\}$. Evidently, it has larger key space 2^{2p} contrast to other methods with only the RCA itself as the key, and can defend exhaustive search attack. For example, if we take $p = 100$, then the key space is at least 2^{200}.

IV. Conclusion

Because of the simple structure of the CA, the system can be simply implemented by VLSI or ASIC, and has high speed contrasted to other methods such as the LFSR due to the high parallel information processing property of the CA. For example, with n cells CA, if p is the number of iteration, then the speed of the encryption is $\frac{n}{p} \times \frac{1}{\Delta T}$, where ΔT is the unit time of the chip of the system. If the number of iteration p is $(n, 2n)$, and lets $\Delta T = 10ns$, then the speed of the system is $50Mbps - 100Mbps$, this is very fast contrast to the approach at present.

References

1. S. Wolfram, Theory and Application of Cellular Automata, World Scientific, Singapore, 1986
2. S. Wolfram, Origins of Randomness in Physical System, Physical Review Letters, Vol.55, No.5, pp.449-452, July 1985.
3. S. Wolfram, Cryptography with Cellular Automata, Advances in Cryptology, pp.429-432, 1985
4. S. Nandi, B. K. Kar, and P. Pal Chaudhuri, Theory and Applications of Cellular Automata in Cryptography, IEEE Trans. Compu., Vol.43, No.12, pp.1346-1356, December 1994
5. P. Guan, Cellular Automata Public-key Cryptosystems, Complex Systems, Vol.1, 1987
6. Farmer D., Toffoli T., and Stephen Wolfram, Cellular Automata, Physica D Vol.10, No.1, 1984
7. S. Wolfram, Statistical Mechanics of Cellular Automata, Review Modern Phys., Vol.55, No.3,

pp.601-644, 1983
8. S. Wolfram, University and Complexity in Cellular Automata, Physica D Vol.10, No.1, 1984
9. Tommaso Toffoli and Norman Margolus, Invertible Cellular Automata: A Review, Physica D Vol.45, pp.229-253, 1990
10. S. Zhang, D. M. Miller, and J. C. Muzio, The Determination of Minimum Cost One-Dimensional Linear Cellular Automata with Maximum Length Cycles, Electronics Letters, Vol.27, No.18, pp.1625-1627, 1991