International Journal of Innovative Computing, Information and Control
Volume **3**, Number **2**, April **2007**

 ISSN 1349-4198
pp. 449–456

DESIGNING OF CHAOTIC SYSTEM OUTPUT SEQUENCE CIRCUIT BASED ON FPGA AND ITS APPLICATIONS IN NETWORK ENCRYPTION CARD

Qun Ding[1,2], Jing Pang[2], Jinqing Fang[3] and Xiyuan Peng[1]

[1]Department of Automatic Test and Control
Harbin Institute of Technology
Harbin 150001, P. R. China
ding-qun@263.net; pxy@hit.edu.cn

[2]Electronic Engineering School
Heilongjiang University
Harbin 150080, P. R. China
Pangjing2002@126.com

[3]China Institute of Atomic Energy
Beijing University of Technology
Beijing 102413, P. R. China
fjq96@126.com

Received January 2006; revised June 2006

Abstract. *Taking the Lorenz chaotic equation as an example, FPGA (Field Programmable Gate Array) technology is applied to obtain chaotic sequence in this paper. Based on the design of a digital integrator and quantification circuit, we get Lorenz chaotic output sequence by DSP Builder tool. This design method may improve arithmetic precision according to the need of the system and resource efficiency. Experiment shows the output sequence of the designed system has good self-correlation. This method can be applied to other continuous chaotic systems and may be applied to chaotic system for information security and secrecy communication field.*
Keywords: FPGA, Lorenz system, Chaos encryption, Self-correlation

1. **Introduction.** With the development of technology, a great change has taken place in the internal structure of communication equipment, computer and test instrument and so on. And discrete components and single chip structures are developing into large scale integrated chip structure and modularization structure. Although system control and complexity of operation are improved continuously, and system function is constantly enhanced, the hardware configuration of systems is becoming simpler and simpler instead and has the eminent characteristics of digital equipment, high stability, high operation accuracy, low failure rate, small volume and so on. Especially when it is combined with computer technique the degree of automation will be highly enhanced. This kind of electronic equipment constituted by a large-scale integrated circuit will be applied more and more and exhibit its superiority in modern economic constructs.

In the information security field, encryption equipment is composed of circuits and arithmetic. It is a modern developing trend of hardware encryption, namely, download the

software programmed encryption arithmetic into a hardware chip. This kind of hardware encryption method possesses the main advantages of the digital equipment introduced above, and besides, the chip programming technology, in which circuit configuration is changed when encryption arithmetic is altered, is much better than the traditional encryption equipment. In addition, the arithmetic rate of a large scale integrated circuit becomes faster and faster, data bus wider and wider, capacity larger and larger and the capability in interfacing with computers stronger and stronger, all the above are applied to electronic information fields widely, and will also have practical potential for applications in information security and secure communication fields and become important means to improving the capability of information security. In large scale integrated circuits, FPGA which takes advantage of its capacity, function and reliance has its wider applications in modern digital equipment. FPGA inherits the merits of ASIC (Application-specific integrated circuit) which is large-scale, high integrated and reliable, and at the same time overcomes the demerits of normal ASIC which is long designed, huge invested and non flexible. It will be preferential to design circuit of complicated digital hardware.

The key technology of information encryption is encryption arithmetic, which has been a research focus and a subject for many scholars [1,5]. Chaotic signal, which is pseudorandom, irreversible and dynamic, is produced by deterministic nonlinear equation. It has good properties of pseudorandom sequence. Chaotic system is very sensitive to initial values, if you set different initial values, the system will run in different orbits whose behavior is difficult to predict. It is of complexity in deterministic nonlinear system, which is adapted for applying to information security and secure communication fields [6,7]. In the process in studying stream cipher arithmetic, it is more difficult to compute chaotic sequence than m-sequence and prediction of initial value is much harder. Besides, it is needed to overcome the disadvantage of m-sequence in which linear arithmetic is easily destroyed. It is significant to apply FPGA technology to realize its cipher in the hardware encryption of information security field and the practical application in chaotic arithmetic.

In this research, we start from two typical chaotic equations, discrete map and continuous chaotic system, which has been studied extensively, and can produce stream cipher respectively. Then, we make relational testing, analysis and comparison of the statistical characteristics for the produced sequence. Some important characteristics, including periodicity, self-correlation, run and equilibrium character, are analyzed for finite sequence. At the same time, corresponding experiments and tests are carried out. All the above will be applied to chaotic system, especially, to establish the base for applications in information security and secure communication fields.

2. **The Produce Method of Lorenz Chaotic Sequence.**

Based on studying the output sequence of one-dimensional discrete chaotic system (Logistic equation)[8], we start our study from an output sequence of a continuous chaotic system. One-dimensional discrete chaotic system has the advantage of its simple form, but it has some advantages, such as short time for producing chaotic sequence and high efficiency in encryption and decryption, its simple structure leads to the secret key space being too small. Low dimensional simple chaotic encryption system has been decoded by Perez [9] and Castillo [10] using phase space reconstruction technique or by way of a neural network. This will be no longer safe to encrypt information by simplex low dimension discrete chaotic

system. But continuous chaotic system has the characteristics including complicated evolution processes and high randomness; it will be much more useful in practices to study encryption.

Lorenz system is a nonlinear three-dimensional differential equation set. Each variable is the function of time t. Lorenz system not only has bifurcation and chaotic phenomena but also diversified stability phenomena, such as multiple periods and stagnant dots. The structure of this kind of chaotic system is complicated and has some system variables and parameters, so it can be used for information security and secure communication fields etc. The well-known Lorenz equation is described by [11]:

$$\begin{cases} \frac{dX}{dt} = 9(Y - X) \\ \frac{dY}{dt} = 35X - Y - 20XZ \\ \frac{dZ}{dt} = 5XY - 1.5Z \end{cases} \tag{1}$$

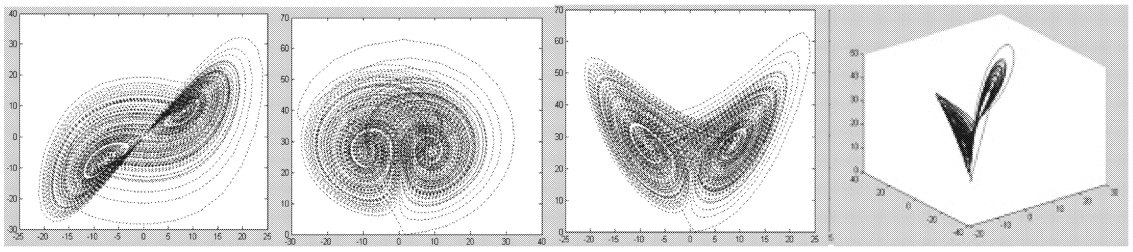
To solve Eq.(1), we use the numerical integral method. Typical phase diagrams and sequential figure for numerical simulation results are shown in Figure 1 and Figure 2.

First of all, we want to use a numerical integral method to get chaotic sequence $x(n)$ from Eq.(1), and then have to change it into binary stream $s(n)$.

Definition 2.1. Quantification function $s(n) = T[x(n)]$ is defined as follows [12]:

$$s(n) = T[x(n)] = \begin{cases} 0 & x(n) \in \bigcup_{k=0}^{2^m-1} I_{2k}^m \\ 1 & x(n) \in \bigcup_{k=0}^{2^m-1} I_{2k-1}^m \end{cases} \tag{2}$$

where $m > 0$ is integer randomly chosen, $I_0^m, I_1^m, I_2^m, \cdots\cdots$ is uniform equal interval in $[0, 1]$. The interval is divided by 2^m. If $x(n)$ is in relevant interval of quantification function then its value is 0 or 1 respectively according to Eq.(2).

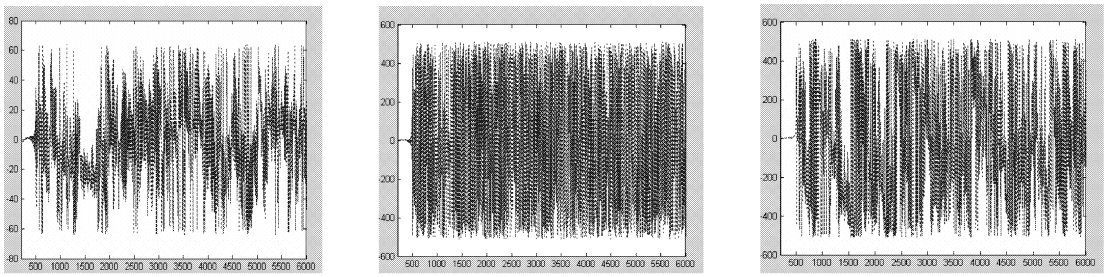


(a) X,Y phase figure (b) Y,Z phase figure (c) X,Z phase figure (d) X,Y,Z phase figure

FIGURE 1. Phase portrait of the modified Lorenz

3. **The Design of Lorenz Chaotic Sequence Circuit.** This circuit is designed by the DSP Builder tool from Altera Company in America. It is based on FPGA [13] and the circuit frame figure is shown in Figure 3.

In the design of Lorenz chaotic sequence, we choose adder, delay, multiplication, amplifier and data selector from the DSP Builder component library and the digital integrator is designed by ourselves. The quantized circuit is made up by barrel shift register and extract bit selector. Using this simple circuit to achieve the quantized function is a trait in designing this circuit. Its principle is described as follows:



(a) X sequential figure (b) Y sequential figure (c) Z sequential figure

FIGURE 2. Time series of the modified

We use the digital integrator introduced above and the components from the DSP Builder component library to construct Lorenz chaotic equation and then in order to make the hardware circuit simple we control the function values of the variables in [0,1]. Firstly the chaotic output signals $x(n)$, $y(n)$ and $z(n)$ are transformed into signals $|x(n)|$, $|y(n)|$, $|z(n)|$ then they are compressed into [0,1].

By sampling value $X = \{\, x(n) \mid n = 0, 1, 2 \cdots\cdots,\ x(n) \in [\,0\,,\ 1]\,\}$, according to quantized function formula (2) , we know that the sequence value after quantized is $S = \{\, s(n) \mid n = 0, 1, 2, \cdots\cdots, s(n) \in \{\,0\,,\ 1\,\}\,\}$, quantized unit $\Delta = 1/2^m$, m is a random integer, quantized interval is $[0\Delta\ \ 1\Delta) \cup [1\Delta\ \ 2\Delta) \cup [2\Delta\ \ 3\Delta) \cdots\cdots \cup [(2^m - 1)\Delta\ \ 2^m\Delta]$ and $k = 0, 1, 2, \cdots\cdots, 2^m - 1$, so the quantized function formula (2) is shown by following formula:

$$s(n) = \begin{cases} 0, & x(n) \in [2k\Delta\ \ (2k+1)\Delta] \\ 1, & x(n) \in [(2k+1)\Delta\ \ (2k+2)\Delta] \end{cases} \tag{3}$$

In order to make the circuit easily achieved then linear transform of formula (3) is applied:

$$s(n) = \begin{cases} 0, & 2^m x(n) \in [2k\ \ \ (2k+1)] \\ 1, & 2^m x(n) \in [(2k+1)\ \ \ (2k+2)] \end{cases} \tag{4}$$

Here the quantized unit is $\Delta = 1$ and the whole quantized interval is $[0\ \ 1) \cup [1\ \ \ 2) \cup [2\ \ \ 3) \cdots\cdots \cup [(2^m - 1)\ \ \ 2^m]$. The quantized interval is determined by the integer bit of $2^m x(n)$, which is determined by parity of the last bit of the integer and the sequence output is 0 or 1, in this way, the hardware circuit can complete the $2^m x(n)$ function only by shift register and parity judgment by bit extractor, then the circuit design can be simplified largely.

Because of the use of the DSP Builder tool, we can realize the system model of the FPGA circuit in Matlab/Simulink and generate hardware description language automatically namely the system is modeled and arithmetically validated in Matlab, after simulation the system can be mapped into a rock-bottom hardware realized scheme based on the FPGA directly, this way of design is simplified

Largely compared to that of tradition, the DSP Builder tool provides the exchange of module AltBus from floating to pointing arithmetic. It can enhance arithmetic precision properly according to the system needs and improve resource utility rate. After the chaotic random sequence is produced, we get the digital circuit types, which are needed, and then it can be downloaded into target hardware. The waveform of three-output logic circuit for the Lorenz system is shown as Figure 4.

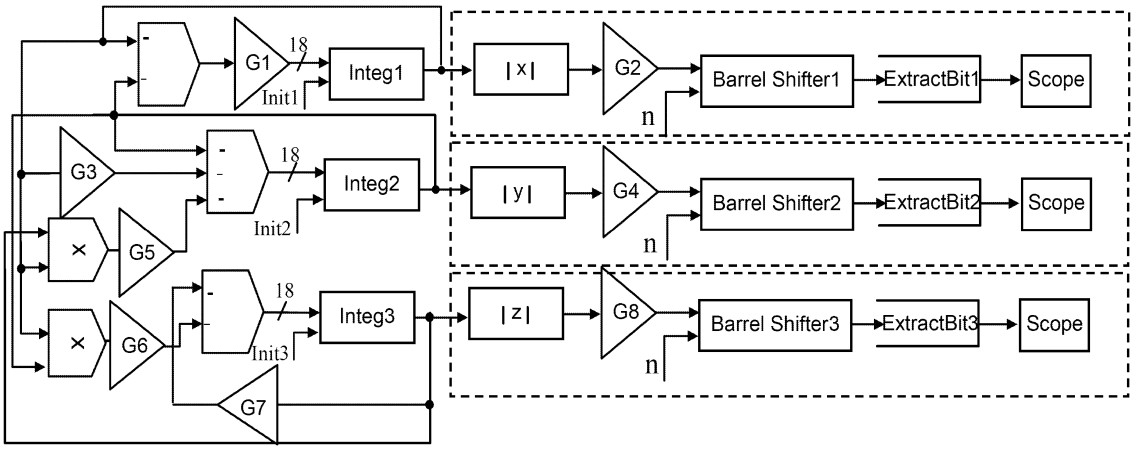


FIGURE 3. Lorenz output sequence circuit frame figure

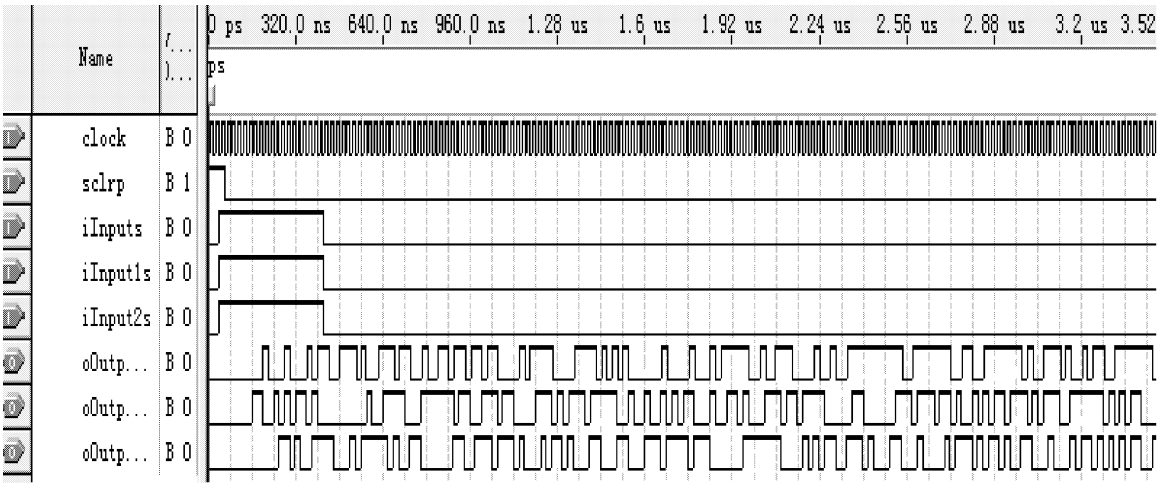


FIGURE 4. The sequential figure of Lorenz

4. **The Test of the Output of the Circuit.** We test the self-correlation and cross-correlation characteristics [14] of the chaotic output sequence that the circuit realized. The way of testing is firstly to change the chaotic sequence into $X = \{\, x(n) \mid n = 0, 1, 2, \cdots\cdots, x(n) \in \{\, -1\,,\, 1\,\}\,\}$ again, then to make the sequence probability density's center from 0.5 to 0. From the analysis of the equilibrium of sequences, we know that after being quantified the numbers of 1s and -1s are almost equal. Thus we can get the estimate formulas for the self-correlation and the cross-correlation function value are as follows, respectively:

The estimate value formula of self-correlation function is

$$R_{XX}(m) = \frac{1}{N} \sum_{n=0}^{N-|m|-1} x(n)\, x(n + |m|) \tag{5}$$

And the estimate value formula of cross-correlation function is

$$R_{XY}(m) = \frac{1}{N} \sum_{n=0}^{N-|m|-1} y(n)\, x(n + |m|) \tag{6}$$

We know that this chaotic sequence has good self-correlation characteristic. When it equals to 0, the peak value is keen-edged. For other values it's nearly zero. Similar to the δ function; if the control parameter is different, it will generate two different sequences and its cross-correlation is very small. These above all can satisfy the needs for cipher sequence, and the self-correlation characteristic of the output sequence is shown in Figure 5.

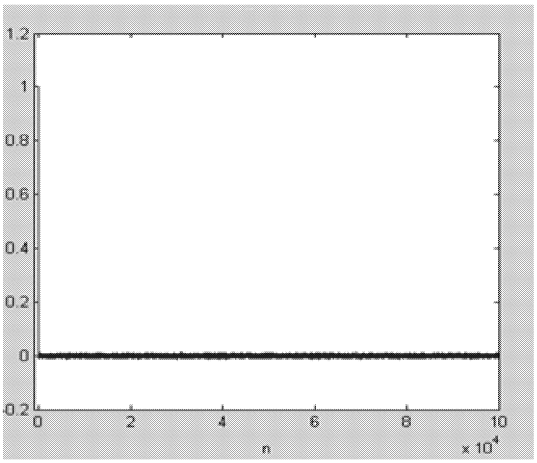


FIGURE 5. Self-correlation characteristic

5. **Possible Applications in Network Encryption Card.** With the rapid development of computer networks and the wider applications of network technology, the data which is transmitted by computer networks is increasing from day to day, but because of the lack of enough safety in actual network systems we cannot avoid the data transmitted by networks being filched and modified which hugely limits the normal application by computer network technology, encryption for network data has been the important subject in information security.

There are a lot of encryption algorithms for network data at present, such as DES algorithm, RSA algorithm, MD5 algorithm and SHA-1 algorithm etc. Most of those algorithms above are public and they are mainly based on software and exist in diversified applications, one way is under the environment of the operation system, the application opens the text which is to be encrypted and uses algorithms to encrypt it and there is another way which is to put the algorithm in the inner signal chip computer for example IC card which can make the encryption algorithm more familiar to the hardware operation speed. But no matter what methods above its core is to band the algorithm in the software environment so the speed of system encrypting data is decided by the work frequency of CPU and we know that the bottle-neck problem exists nowadays is that the work frequency of CPU limits certain time encryption of large capacity data stream, and besides, many filches use special methods to get the encryption algorithm of software

which can affect the security and high-speed real time communication, but compared to traditional software encryption, the characteristic of hardware encryption is using the design idea of software programs to generate hardware logic which encryption algorithm is completely hardened in hardware logic gate circuit , so the problem that the speed of serial work of CPU is limited is solved. The encryption speed is enhanced, and besides, the encryption algorithm can be updated at any time which is hard to decode by traditional decryption mode.

This network encryption card which is composed of three parts, FPGA encryption chip, RAM chip and network interface chip is based on the FPGA and chaotic sequence as the core algorithm (the functional block diagram is shown in Figure 6). Here the FPGA encryption chip integrates PCI interface module and Lorenz encryption module in which Lorenz encryption module performs for encryption process for the data coming from one of the three Lorenz sequences and the data coming from the PCI interface according to the bits, PCI interface module can realize work clock, the interfaces of bus, the read and write of internal storage space and PCI interrupt function. This network encryption card integrates chaotic stream cipher into a chip and enhances the security of the network system.

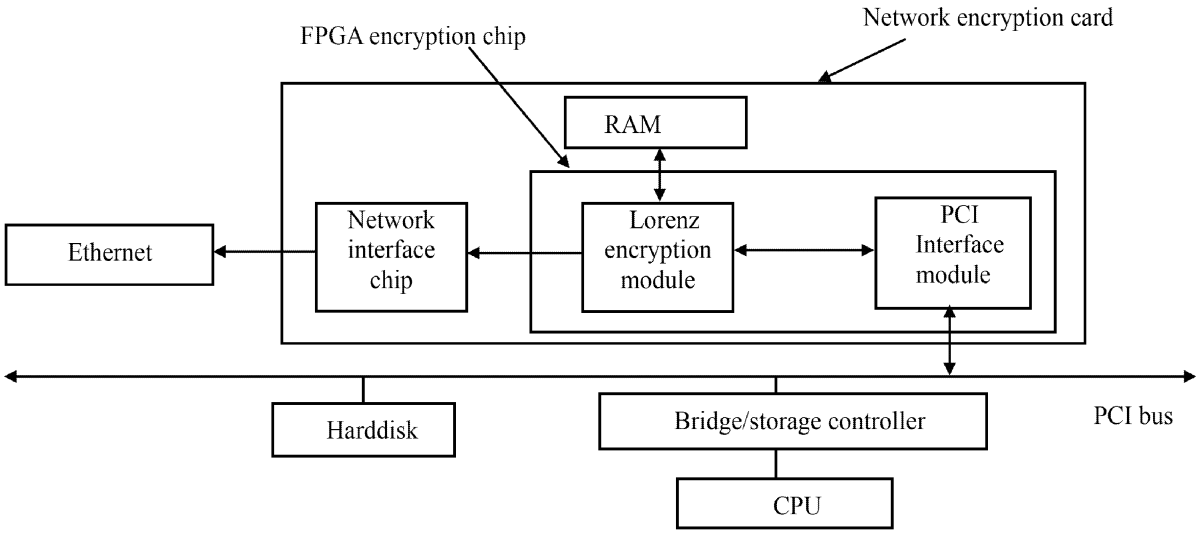


FIGURE 6. Functional block diagram of network encryption card

6. **Conclusions.** This paper mainly introduces a method for realizing continuous chaotic output sequence by FPGA technology and the supernatural characteristics of chaos by modern circuit design methods. It can improve the finite precision affect in practical computation. The Lorenz circuit and sequence generator are designed in the form of a simple circuit. It can save hardware resources at the same time and enhance the practicability. The output sequence of the circuit can reach the basic pseudo-random characteristic. This idea and method can be extended to generate other chaotic sequence circuits. We can design an encryption chip, which may be applied to secure communication and information security fields.

Acknowledgements. This work was supported by the National Science Foundation of China (No.60672011).

REFERENCES

[1] Zhao, G. and J. Fang, The evolvement of the application of modern information security and chaotic secure communication study, *The Evolvement of the Physics*, vol.23, no.2, pp.212-252, 2003.

[2] Li, S., X. Mou and Y. Cai, Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography, *Proc. of the Second International Conference on Cryptology*, India, pp.316-329,2001.

[3] Yen, J.-C. and J.-I. Guo, Efficient hierarchical chaotic image encryption arithmetic and its VLSI realization, *Proc. of the IEE on Image Signal Process*, vol.147, no.2, 2000.

[4] Dachselt, F. and W. Schwarz, Chaos and cryptography, *IEEE Transactions on Circuits and System: Fundamental Theory and Applications*, vol.48, no.12, pp.1498-1509, 2001.

[5] Li, K., Y. C. Soh and Z. G. Li, Chaotic cryptosystem with high sensitivity to parameter mismatch, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol.50, no.4, pp.579-583, 2003.

[6] Wang, X., *The Chaos in Complex Nonlinear System*, Electronic Industry Press, Beijing, 2003.

[7] Huang, R., *Chaos and Its Application*, Wuhan University Press, Wuhan, 2003.

[8] Ding, Q., Y. Zhu, F. Zhang and X. Peng, Discrete chaotic and the property analysis of output sequence, *Proc. of the International Symposium on Communications and Information Technologies*, Beijing, China, vol.2, pp.1009-1012, 2005.

[9] Perez, G. and H. A. Gerdeira, Extracting messages masked by chaos, *Phys Rev Lett*, vol.74, pp.1970-1973, 1995.

[10] Castillo, E. and J. M. Gutierrez, Nonlinear time modeling and prediction using functional networks, *Physics Letters A*, vol.244, pp.71-84, 1998.

[11] Sobhy, M. I., M. A. Aseeri and A. E. R. Shehata, Real time implementation of continuous (Chua and Lorenz) chaotic generator models using digital hardware, *Proc. of the Third International Symposium on Communication Systems Networks and Digital Processing*, pp.38-41, 2002.

[12] Qiu, H., C. He and H. Zhu, A kind of infinite collapsed chaos mapping and its quantized sequence, *Journal of Shanghai Jiao Tong University* ,vol.36, no.12, pp.1788-1790, 2002.

[13] Pan, S., J. Huang and G. Wang, *Modern DSP Technology*, Xidian University Press, Xian, 2003.

[14] Zheng, W., *Randam Signal Analysis*, Harbin Institute of Technology Press, Harbin, 1999.