Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009

A NEW CLASS OF EFFICIENT PIECEWISE NONLINEAR CHAOTIC MAPS FOR SECURE CRYPTOSYSTEMS

YONG-KUI LI[1], QIAO-SHENG FENG[1], WAN-QUAN LIU[2], YUN-QIONG WANG[1]

[1]Institute of Computer Science and Information Technology, Yunnan Normal University, Kunming 650092, P. R. China
[2]Department of Computing, Curtin University of Technology, Perth, Australia
E-MAIL: lyk0@163.com, w.liu@curtin.edu.au, fengqs@public.km.yn.cn, wyunqiong@sina.com

Abstract:

In this paper we construct a new class of nonlinear chaotic maps for secure cryptosystems. These maps can overcome the security holes brought by the "piecewise linearity" of the previous Piecewise Linear Chaotic Maps (PWLCM) due to a fact that the chaotic sequences generated by the derived iterative system based on the proposed maps are proved to have perfect dynamic properties, such as uniform invariant distribution, δ-like autocorrelation function etc. Furthermore, the relative quantized two-value sequences also have perfect secure statistical characteristics. In terms of computing speed, the proposed maps have faster speed than the recently proposed nonlinear "piecewise-square-root" maps (PSRM), and they actually have equivalently the same computing speed with the linear PWLCM.

Keywords:

Chaotic maps; Nonlinear maps; Cryptography; Invariant distribution

1. Introduction

Recently it is an attractive research trend to apply the chaos theory and techniques to cryptography, in which many new cryptosystems and algorithms have been proposed. At the same time many corresponding attack methods for the proposed systems are designed in order to test their security. In the developed cryptosystems, PWLCM is a popular one, which can be easily implemented while satisfying many excellent dynamical properties compared with Logistic maps [1]. For example, the invariant distribution of the signals generated by iterating Logistic maps is not a uniform function and there are many period windows to different parameters in them. Actually, PWLCM is a class of chaotic maps used in many cryptosystems [2-6]. However, cryptosystems based on these maps have potential security threat due to their "piecewise linearity" defects. Some of them have been attacked successfully by linear prediction or reconstruction. For example, Habutsu [7] suggested a cryptosystem based on iterating PWLCM, but immediately Biham [8] proposed a chosen cipher-text attack and a known plaintext attack to the cryptosystem. In order to address the security defect issue properly, four basic properties, which the chaotic two-value sequences in cryptosystems should satisfy, are proposed in [9] and they are as follows: *a*) have an enough long period; *b*) have δ-like autocorrelation function, zero cross correlation function, independent and identical binomial distribution; *c*) have an ideal linear complexity for fast computing speed; *d*) have nonlinear property, namely the maps should have no linear property in order to resist any possible linear prediction or reconstruction attack. Obviously, PWLCM don't possess the last property above. In order to achieve these aims, a new class of nonlinear chaotic maps called "piecewise-square-root" maps is proposed in [10]. The proposed maps can conquer the security defects and satisfy the four properties above. However, one obvious deficiency is that their implementation needs square root floating-point operations and this is not in favor of fast computation for the encrypting and decrypting systems. So, it is only suitable to use these maps when the computational cost in implementing the system is not a significant factor as mentioned in [11]. Based on such observation, some efficient nonlinear maps are still required for some cryptosystems in order to reduce the computational cost. In this paper we will construct a new class of efficient piecewise nonlinear chaotic maps for efficiency purpose and their corresponding properties will be analyzed. The theoretic analysis and experimental testing show that these maps can achieve better results than those in [10].

2. The New piecewise Nonlinear Chaotic Maps and Their Properties

The chaotic two-value sequences used in the cryptosystems can be generated by a real number analog chaotic sequences based on a discrete-time iterative system

978-1-4244-3703-0/09/$25.00 ©2009 IEEE

$x_{t+1}=F(x_t)$. If these two-value sequences are used as keys in secure cryptosystems, they should satisfy the four properties mentioned in previous section. The property *a*) can be satisfied via the method of perturbation [12, 13]; the property *b*) and *c*) can be satisfied by the chaotic maps and their quantizing function. The chaotic maps constructed in this paper can also satisfy the nonlinear property and have some perfect dynamical properties. For example, the probability density function (PDF) of the output signals derived from the maps is a uniform distribution, and their autocorrelation function is a δ -like function, etc.

2.1 The New Chaotic Nonlinear Maps

In order to achieve more secure and high efficiency cryptosystems, we propose the following new piecewise nonlinear chaotic maps:

$$F(x)=\begin{cases} 1-(p_i-x)\left[\left(\dfrac{2}{p_i-\dfrac{2i-2}{n}}-n\right)\dfrac{\dfrac{2i-2}{n}+a_{2i-1}}{x+a_{2i-1}}+n\right], & x\in\left[\dfrac{2i-2}{n},p_i\right) \\ 1-\left(\dfrac{2i}{n}-x\right)\left[\left(\dfrac{2}{\dfrac{2i}{n}-p_i}-n\right)\dfrac{p_i+a_{2i}}{x+a_{2i}}+n\right], & x\in\left[p_i,\dfrac{2i}{n}\right) \\ 1, & x=1 \\ F(-x), & x<0 \end{cases} \tag{1}$$

In Eq. (1), $\theta=[-1,1]$, $x\in\theta$; $n\geqslant 2$ and n is an even number; $1\leqslant i\leqslant n/2$ and $i\in N$; $\dfrac{2i-2}{n}<p_i<\dfrac{2i}{n}$. The parameters $\{a_1, a_2, \cdots\cdots, a_n\}$ satisfy the following constraint conditions.

$$\begin{cases} a_{2i-1}<-p_i \quad or \quad a_{2i-1}>-\dfrac{2i-2}{n} \\ a_{2i}=-\dfrac{\left(\dfrac{2i}{n}-p_i\right)a_{2i-1}+\dfrac{2p_i}{n}}{\left(p_i-\dfrac{2i-2}{n}\right)} \end{cases} \tag{2}$$

2.2 The Properties for the Proposed Maps

For the proposed maps in (1) we prove that they have the following properties.

Theorem With the given nonlinear maps in (1), we have the following properties.

(a) The iterative system $x_{t+1}=F(x_t)$ ($t\geqslant 0$ and $t\in Z$) is chaotic;

(b) The iterative output signals $\{x_t\}_{t=1}^{\infty}$ are ergodic on θ and their invariant distribution is a uniform distribution, and the corresponding PDF is

$$f(x)=\begin{cases} 0.5, & x\in\theta \\ 0, & others \end{cases}.$$

(c) The sequences $\{x_t\}_{t=1}^{\infty}$ has δ -like autocorrelation function, namely,

$$\rho_F(r)=\frac{\lim\limits_{J\to\infty}\dfrac{1}{J}\sum\limits_{t=1}^{J}x_t x_{t+r}}{\lim\limits_{J\to\infty}\dfrac{1}{J}\sum\limits_{t=1}^{J}(x_t)^2}=\delta(r),\quad r\in Z.$$

Proof: First one notices that if $\dfrac{2i-2}{n}\leq x<p_i$, then the map equation can be rewritten as

$$F_{2i-1}(x)=nx-\frac{b_{2i-1}}{x+a_{2i-1}}+c_{2i-1},$$

where

$$b_{2i-1}=\left(\frac{2}{p_i-\dfrac{2i-2}{n}}-n\right)\left(a_{2i-1}+\frac{2i-2}{n}\right)(a_{2i-1}+p_i)>0,$$

$$c_{2i-1}=\left(\frac{2}{p_i-\dfrac{2i-2}{n}}-n\right)\left(a_{2i-1}+\frac{2i-2}{n}\right)+1-np_i;$$

If $p_i\leq x<\dfrac{2i}{n}$,

$$F_{2i}(x)=nx-\frac{b_{2i}}{x+a_{2i}}+c_{2i},$$

where

$$b_{2i}=\left(\frac{2}{\dfrac{2i}{n}-p_i}-n\right)(a_{2i}+p_i)\left(a_{2i}+\frac{2i}{n}\right)>0,$$

$$c_{2i}=\left(\frac{2}{\dfrac{2i}{n}-p_i}-n\right)(a_{2i}+p_i)+1-2i.$$

Next we prove part (a).

a) When $\dfrac{2i-2}{n}\leq x<p_i$,

$$\left|F'(x)\right|=n+\frac{b_{2i-1}}{(x+a_{2i-1})^2}>n;$$

when $p_i\leq x<\dfrac{2i}{n}$,

$$\left|F'(x)\right|=n+\frac{b_{2i}}{(x+a_{2i})^2}>n.$$

Since $F(x)$ is symmetry for all $x\in\theta$, so $\left|F'(x)\right|>n$. Then from the definition of the Lyapunov exponent [14] we know that

$$\lambda=\lim_{J\to\infty}\frac{1}{J}\log_2\left[\prod_{t=1}^{J}\left|F'(x_t)\right|\right]>\log_2 n\geq 1,$$

The positive value λ indicates that the iterative

system is chaotic [14].

b) Since

$$F(x) = nx - \frac{b}{x+a} + c, \quad b > 0 ,$$

So,

$$\frac{|F''(x)|}{(F'(x))^2} = \frac{2b|(x+a)^{-3}|}{(n + b/(x+a)^2)^2} = \frac{2b}{|x+a|(n(x+a)+b/(x+a))^2} ,$$

If $x+a>0$ or $x+a<0$, then

$$(n(x+a)+b/(x+a))^2 \geq (2\sqrt{bn})^2 = 4bn ,$$

Therefore

$$\frac{|F''(x)|}{(F'(x))^2} \leq \frac{1}{2n|x+a|} .$$

So when

$$\frac{2i-2}{n} \leq x < p_i ,$$

If $a_{2i-1} < -p_i$, then

$$x + a_{2i-1} < x - p_i < 0 ;$$

If $a_{2i-1} > -\frac{2i-2}{n}$, then

$$x + a_{2i-1} > x - \frac{2i-2}{n} \geq 0 .$$

So

$$\frac{|F''(x)|}{(F'(x))^2} \leq \frac{1}{2n|x+a_{2i-1}|} < +\infty ;$$

When $p_i \leq x < \frac{2i}{n}$,

If $a_{2i-1} < -p_i$, from the condition (2) we know

$$a_{2i} > -p_i , \quad x + a_{2i} > x - p_i \geq 0 ;$$

If $a_{2i-1} > -\frac{2i-2}{n}$, from the condition (2) we know

$$a_{2i} < -\frac{2i}{n} ,$$

$$x + a_{2i} < x - \frac{2i}{n} < 0 ,$$

So

$$\frac{|F''(x)|}{(F'(x))^2} \leq \frac{1}{2n|x+a_{2i}|} < +\infty .$$

Since *F(x)* is symmetry for all $x \in \theta$, so

$$\frac{|F''(x)|}{(F'(x))^2} < +\infty .$$

Then from [15] we know that the "iterative output signals $\{x_t\}_{t=1}^{\infty}$ are ergodic on θ and their exclusive PDF *f(x)* satisfy $f(x) = P_r^{\circ} f(x)$ ". Here *Pr* is Frobenius-Perron operator defined as

$$P_r^{\circ} f(x) = \frac{d}{dx}\int_{F^{-1}([-1,x])} f(x)dx .$$

Let

$$y=F(x),\ x=F^{-1}(y),$$

When

$$\frac{2i-2}{n} \leq x < p_i ,$$

We will have

$$\left(F_{2i-1}^{-1}(x)\right)' = \frac{1}{2n} \pm \frac{x + na_{2i-1} - c_{2i-1}}{2n\sqrt{(x + na_{2i-1} - c_{2i-1})^2 + 4nb_{2i-1}}} ,$$

If $a_{2i-1} < -p_i$, then one takes the positive sign, if $a_{2i-1} > -\frac{2i-2}{n}$ then one takes the negative sign;

When $p_i \leq x < \frac{2i}{n}$,

$$\left(F_{2i}^{-1}(x)\right)' = \frac{1}{2n} \mp \frac{x + na_{2i} - c_{2i}}{2n\sqrt{(x + na_{2i} - c_{2i})^2 + 4nb_{2i}}} ,$$

If $a_{2i} > -p_i$ then one takes the negative sign, if $a_{2i} < -\frac{2i}{n}$ then one takes the positive sign; From the condition (2), we know that

$$na_{2i-1} - c_{2i-1} = na_{2i} - c_{2i} , \quad b_{2i-1} = b_{2i} .$$

And when $a_{2i-1} < -p_i$, then $a_{2i} > -p_i$; when $a_{2i-1} > -\frac{2i-2}{n}$, then $a_{2i} < -\frac{2i}{n}$. So when adding the two items, one can see that the positive item just counteract with the negative item, namely, when $\frac{2i-2}{n} \leq x < \frac{2i}{n}$, we have

$$\left(F_{2i-1}^{-1}(x)\right)' + \left(F_{2i}^{-1}(x)\right)' = 1/n ,$$

So in the case of these maps, the Frobenius-Perron operator is

$$P_r^{\circ} f(x) = \sum_{i=1}^{n/2} \left([f(y_{2i-1}) + f(-y_{2i-1})]\left(F_{2i-1}^{-1}(x)\right)' + [f(y_{2i}) + f(-y_{2i})]\left(F_{2i}^{-1}(x)\right)' \right)$$

where

$$y_{2i-1} = \left(x - na_{2i-1} - c_{2i-1} \pm \sqrt{(x + na_{2i-1} - c_{2i-1})^2 + 4nb_{2i-1}}\right) \Big/ 2n ,$$

$$y_{2i} = \left(x - na_{2i} - c_{2i} \pm \sqrt{(x + na_{2i} - c_{2i})^2 + 4nb_{2i}}\right) \Big/ 2n .$$

Then we can derive that with condition (2), the PDF of the maps in (1) is

$$f(x)=0.5,\ x \in \theta ,$$

and it is the unique solution which satisfies $f(x) = P_r^{\circ} f(x)$, so the property (b) is proved.

c) Since $\{x_t\}_{t=1}^{\infty}$ is ergodic on θ and its invariant distribution is uniform distribution, we can rewrite their autocorrelation function as:

$$\rho_F(r) = \int_{-1}^{1} xF^r(x)f(x)dx \Big/ \int_{-1}^{1} x^2 f(x)dx , \quad r \geq 0 \ \ and \ \ r \in Z .$$

When r=0,

$$F^r(x)=x, \quad \rho_F(x)=1;$$

When $r \geqslant 1$ and $r \in Z$, $F^r(x)$ is an even function, but x is an odd function. So

$$\rho_F(x)=0;$$

When $r \leqslant -1$ and $r \in Z$, let $t+r=s$, then

$$\rho_F(r)=\frac{\lim_{J\to\infty}\frac{1}{J}\sum_{s=1+r}^{J+r} x_s x_{s-r}}{\lim_{J\to\infty}\frac{1}{J}\sum_{s=1+r}^{J+r}(x_{s-r})^2},$$

i.e.,

$$\frac{\int_{-1}^{1} xF^{-r}(x)dx}{\int_{-1}^{1}\left(F^{-r}(x)\right)^2 dx}.$$

$F^r(x)$ is an even function, but x is an odd function, then $\rho_F(x)=0$. The property (c) is proved.

In order to satisfy the application requirements in secure digital communication, we can quantize the above iterative signals into 0-1 two-value sequences according to the method in [10]. Then the two-value sequences quantized by irreversible transforms also have perfect security statistic characteristics theoretically, such as balanced 0-1 rate, δ-like autocorrelation function, zero cross correlation function of different sequences, independent and identical binomial distribution, ideal linear complexity and nonlinear complexity and so on. These discussions are similar to [10] and thus are omitted here.

3. Analysis and Comparison with PWLCM and PSRM

The chaotic sequences generated by these three chaotic maps (the proposed maps in this paper, PWLCM and PSRM) all have perfect chaotic dynamical properties, i.e., they all have the invariant uniform distribution, and their autocorrelation function is δ-like function. And also all the quantized two-value sequences have perfect security statistic characteristics. However, they also have significant differences. The PWLCM has very fast computing speed because of their simple linear forms, but the cryptosystems designed with the PWLCM have the security defects due to its "piecewise linearity". The PSRM satisfy nonlinear property and can conquer the security defects, but the square root floating-point operations in these maps make the fast implementation impossible or difficult when encrypting and decrypting information [11]. The proposed piecewise nonlinear chaotic maps in this paper resolved this conflict, namely, they are "piecewise nonlinear", which can overcome the security problem brought by "piecewise linearity". Moreover, there are only four arithmetic operations in the implementation of these maps like the PWLCM. Table 1 shows the average operations of different operators in the three maps when calculating the sequences for one segment. So the proposed maps have similar operations as PWLCM and have no square root operation. The experiments in next section will show that they will be much faster than the PSRM and close to the speed of PWLCM.

Table 1. The average calculating times of different operators in the three maps

	+	-	*	/	$\sqrt{\ }$
PWLCM	0	3	1	1	0
The new maps	3	3	2	2	0
PSRM	0	5	3	2	1

4. Illustrative Examples

4.1. Validation for the Properties of the Proposed Nonlinear Maps

In this section we do some experiments to validate the important properties of the new chaotic maps proved in previous section. In the experiments for all the three maps, we let the map interval be [-1, 1] with n = 2. Also we set the same segmentation point value

$$p = 0.28495469875412,$$

with the same initial value

$$x_0 = 0.78392236547856.$$

In the proposed maps and the PSRM, we set the parameter a_1 = 0.56784569324568. Then Figure 1 shows the PDFs of the three generated sequences by iterating 10^7 times and Figure 2 shows the autocorrelation functions of the three sequences by iterating 10^3 times, where the green line is for the PSRM, the red one is for the new maps and the blue one is for the PWLCM. One can see from these figures that the proposed nonlinear chaotic maps possess the perfect dynamical properties like PWLCM and PSRM.

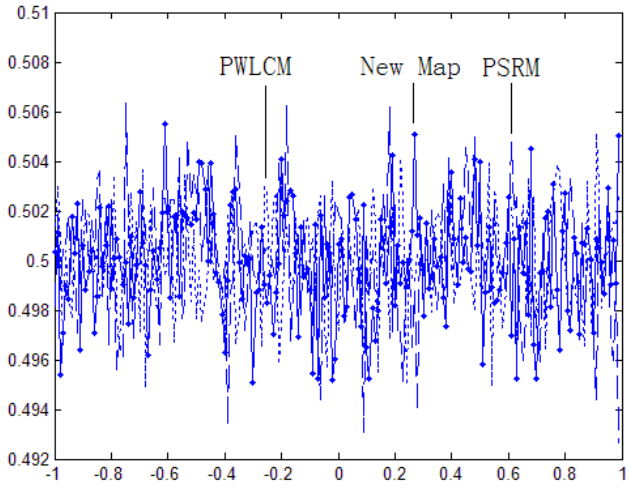

Figure 1. The PDFs of sequences when iterating 10^7 times

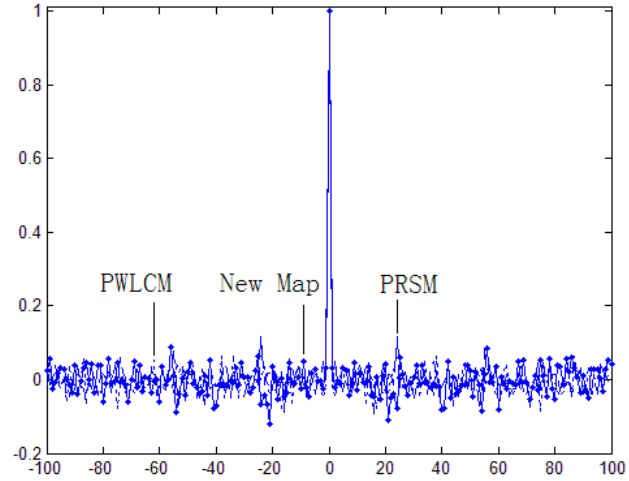

Figure 2. The sequences generated from autocorrelation functions when iterating 10^3 times

To conquer the short period effect of the chaotic sequences when implementing the systems with finite precision, we can employ the method of perturbation by m-sequences and get the chaotic sequences whose periods are long enough as discussed in [12, 13]. Then we can generate two-value sequences quantized by irreversible transforms and apply them to cryptography.

4.2. Validation for the Computing Performance

The experiments in this section will validate the advantages of the new chaotic maps for computing performance. In the same software and hardware configuration environment, namely the CPU clock speed is 1.5GHz, the memory size is 512MB with the software Matlab 7.1. We let all the map interval be [-1, 1], and set the same segmentation point value p with the same initial value x_0. For the new maps, the PSRM and the PWLCM maps we set all the parameters as in section 3.1. Then we separately iterate 10^6, $5*10^6$, 10^7, $5*10^7$ times, calculate the CPU escaped time (the unit is second) for all the chaotic maps in the same condition, and then we get the experiments results in Table 2. Eq. (3) is the equation of the new map when n=2, and its corresponding condition is Eq. (4).

$$F(x)=\begin{cases}1-2(p-x)\left[\dfrac{(1-p)a_1}{p(x+a_1)}+1\right], & x\in[0,p)\\ 1-2(1-x)\left[\dfrac{p(p+a_2)}{(1-p)(x+a_2)}+1\right], & x\in[p,1)\\ 1, & x=1\\ F(-x), & x<0\end{cases} \tag{3}$$

$$\begin{cases}a_1<-p \quad or \quad a_1>0\\ a_2=(1-1/p)a_1-1\end{cases} \tag{4}$$

Table 2. The CPU escaped time of all the chaotic maps with the same condition (the unit is second)

	10^6	$5*10^6$	10^7	$5*10^7$
PWLCM	0.8281	4.0469	8.2813	43.2031
The new maps	0.8594	4.2500	8.4375	45.1406
PSRM	12.0938	60.3125	120.6563	614.2031

We can see from Table 2 that the iterative calculation speed of the proposed maps is 13-15 times faster than the PSRM, and is similar to the PWLCM. Further one can notice that there is one more parameter a_1 in the proposed maps than the PWLCM. This validates our conclusion the proposed maps have secure property due to nonlinearity but have similar computing performance with linear PWLCM maps. The main advantage for the proposed maps is that the square-root operation is avoided for reduction of computational cost. Observing the Figure 2 and table 2, we have the following remarks.

Remarks: (i) From Figure 2, we can observe that the proposed chaotic maps will produce larger sparks when they generate the autocorrelation functions compared to the PWLCM and PSRM. This will provide more randomness for the sequences, leading to more secure cryptosystems.

(ii) From Table 2, we notice that the proposed maps will run much faster than the PSRM, this is mainly due to a fact that the square root operation is not used in the proposed maps.

5. Conclusions

A new class of piecewise nonlinear chaotic maps is proposed in this paper which can conquer the security defects brought by the "piecewise linearity". However they

can have nearly the same computing performance with the linear PWLCM and this has obvious advantages than the "piecewise-square-root" maps. So these new chaotic maps can be applied to the design of cryptosystems with high requirements in security and computing efficiency and they can replace PWLCM for security and the "piecewise-square-root" maps for efficiency.

References

[1] Gonzalo Alvarez and Shujun Li, "Some basic cryptographic requirements for chaos-based cryptosystems" *Int. J. Bifurcation and Chaos* 16, 2129–2151, 2006.

[2] Shujun Li, Xuanqin Mou, and Yuanlong Cai, "Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography," *In Progress in Cryptology INDOCRYPT, Lecture Notes in Computer Science* vol. 2247, pages 316–329. Springer-Verlag, Berlin, 2001.

[3] Xun Yi, Chik How Tan, and Chee Kheong Siew, "A new block cipher based on chaotic tent maps," *IEEE Trans. Circuits and Systems–I*, 49(12): 1826–1829, 2002.

[4] Naoki Masuda and Kazuyuki Aihara, "Cryptosystems with discretized chaotic maps," *IEEE Trans. Circuits and Systems–I*, 49(1): 28–40, 2002.

[5] Hong Zhou and Xieting Ling, "Generating chaotic secure sequences with desired statistical properties and high security," *Int. J. Bifurcation and Chaos*, 7(1): 205–213, 1997.

[6] Mieczyslaw Jessa, "Data transmission with adjustable security exploiting chaos-based pseudorandom number generators," *In Proc. IEEE Int. Symposium Circuits and Systems*, volume III, pages 476–479. IEEE, 2002.

[7] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and Shinsaku Mori, "A secret key cryptosystem by iterating chaotic map," *Lecture notes in computer science, Advances in cryptology*, proceedings of EUROCRYPT' 91, pp. 127-140, 1991.

[8] E. Biham, "Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT' 91," *Advances in Cryptology-DUROCRYP'* 91, Berlin Heideberg: Springer-Verlag, pp. 532~534, 1991.

[9] Schuneier, Applied Cryptography. New York: John Wiley, 347~374, 1994.

[10] Sang Tao, Wang Ruli, and Yan Yixun, "The theoretical design for a class of new chaotic feedback stream ciphers," *Chinese Journal of Electronics*, 27(7): 47-50, 1999.

[11] Li, S, "Analyses and New Designs of Digital Chaotic Ciphers," *PhD thesis, School of Electronics and Information Engineering*, Xi'an Jiaotong University, Xi'an, China, 2003, available online at http://www.hooklee.com/pub.html.

[12] Zhou Hong, and Ling Xieting, "Realizing finite precision chaotic systems via perturbation of m-sequences," *Chinese Journal of Electronics*, 1997, 25(7): 95~97.

[13] Zhou Hong, Luo Jie, and Ling Xieting, "Generating nonlinear feedback stream ciphers via chaotic systems," *Chinese Journal of Electronics*, 1997, 25(10): 57~60.

[14] Ch. Mira, Chaotic Dynamics, Singapore: World Scientific, 1987: 2~81

[15] S. Grossmann and S. Thomae. Z, Naturforsch, "Invariant distributions and stationary correlation functions of one-dimensional discrete processes," *Zeitschrift Naturforschung* Teil A, Vol. 32, p. 1353. 1977, 32(a): 1353-1363.