Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2012, Article ID 619257, 12 pages
doi:10.1155/2012/619257

Research Article

Theorem to Generate Independently and Uniformly Distributed Chaotic Key Stream via Topologically Conjugated Maps of Tent Map

Zheng guang Xu,[1] Qing Tian,[1] and Li Tian[2]

[1] *Department of Control Science and Engineering, School of Automation, University of Science and Technology Beijing, Beijing 100083, China*
[2] *Department of Control Science and Engineering, School of Astronautics, Beijing University of Aeronautics and Astronautics, Beijing 100191, China*

Correspondence should be addressed to Qing Tian, qingtiantq@hotmail.com

Received 26 July 2012; Revised 4 October 2012; Accepted 16 October 2012

Academic Editor: Kwok-Wo Wong

This paper proposes a theorem to generate chaotic key stream from topologically conjugated maps of Tent Map. In this theorem, the condition for topological conjugation between Tent Map and a class of chaotic maps is first determined. Then, the chaotic attractor of the maps is divided into 2^n unequal subintervals, the chaotic orbit is sampled once in n time iteration, and, finally, the independently and uniformly distributed 2^n phase key stream is obtained. The theoretical and numerical analyses show that the chaotic key stream generated by the proposed theorem successfully is independent and uniform, has a certain complex degree close to the maximum approximate entropy for 2^n phase key stream, and satisfies the randomness requirement defined in NIST SP800-22. This theorem can be used in fields such as cryptography and numerical simulation.

1. Introduction

Random number generation is very important in cryptography, especially in key construction. In symmetric and asymmetric cryptosystems, the random number is the primary resource for key generation. Further, random number generators (RNGs) are used to create challenges, nonce, padding bytes, and blinding values in many cryptographic protocols.

There are two basic types of generators that produce random sequences: true random number generators (TRNGs) [1] and pseudorandom number generators (PRNGs) [2–5]. PRNGs are generally faster than TRNGs, and, therefore, PRNGs are preferable in applications requiring a large number of random numbers.

Chaotic system, characterized by sensitive dependence on initial conditions, similarity to random behavior, continuous broad-band power spectrum, inherent determinism, and simplicity of realization, can be potentially exploited for PRNGs [6, 7]. Most applications of chaotic maps use a one- or multidimensional chaotic map as a PRNG to produce a binary stream, which is then XORed with the plaintext to produce the cipher-text [8–11]. Thus, the statistical property—independently and identically distributed (IID)—of chaotic key stream plays an important role in avoiding cipher-text attacking.

Tent Map is described by the uniform probability law, and, hence, the statistical independence of successive binary symbols is the main problem to be addressed. Some studies focus on experiments that determine the selection of a suitable Tent Map parameter for different applications where the statistical independence is of interest. The relationship between the Tent Map parameter and the statistical independence decision is indicated in [12]. Complying with the fair coin tossing model in [13], the threshold is given according to the Tent Map parameter to obtain a statistically independent key stream. Other studies have focused on theoretical proofs. Logistic Map is topologically conjugated with Tent Map [14], and, therefore, Hu et al. proposed a method for generating chaotic key stream based on Logistic Map [15]. This key stream is proved to be independent and uniform. AdrianLuca and Vlad provided another method for generating IID samples using Logistic Map by combining discrete noisy channel with the test of independence in contingency tables [16]. Until now, the research for generating IID key stream by topological conjugation has been limited to Logistic Map. However, in our study, we determine a more general condition, under which a class of chaotic systems can produce the IID key stream. Meanwhile, the proof in [14] can be considered as the example for the theorem proposed in this paper.

2. Theorem for Generation of IID Key Streams

In this section, we specify the conditions and process required for a class of topologically conjugated mapping systems of Tent Map to generate the IID key stream.

Definition 2.1 (see [17]). For two one-dimensional maps,we have

$$\begin{aligned} x_{k+1} &= g(x_k), \quad x \in I \subset R, \\ y_{k+1} &= g(y_k), \quad x \in J \subset R. \end{aligned} \tag{2.1}$$

If there exists a continuous and invertible map $h : I \to J$, such that $y_k = h(x_k)$, making $h^{-1} \circ f \circ h(x_k) = g(x_k)$ and $h \circ g \circ h^{-1}(y_k) = f(y_k)$, then f and g are said to be topologically conjugated via h.

Lemma 2.2 (see [17]). *If f and g are topologically conjugated via h, then f^n and g^n are topologically conjugated via h.*

Lemma 2.3 (see [17]). *If f and g are topologically conjugated via h, and ρ_g is the probability density function of g, then the probability density function of f is*

$$\rho_f(x) = \rho_g\left(h^{-1}(x)\right)\left|\frac{dh^{-1}(x)}{dx}\right|. \tag{2.2}$$

Theorem 2.4. *For tent map, we have*

$$x_{k+1} = g(x_k) = \begin{cases} 2x_k, & 0 \leq x_k \leq \dfrac{1}{2} \\ 2 - 2x_k, & \dfrac{1}{2} \leq x_k \leq 1 \end{cases} \tag{2.3}$$

when $ma = -4$, and $m, a \in R$,

$$f(x_k) = mx_k^2 + 4x_k, \quad x_k \in [\min\{0,a\}, \max\{0,a\}], \tag{2.4}$$

and $g(x_k)$ are topologically conjugated via

$$h(x_k) = a\sin^2\frac{\pi x_k}{2}, \quad a \neq 0. \tag{2.5}$$

For the map $f(x_k) = mx_k^2 + 4x_k$ defined by (2.4), we choose n as sampling step, that is, $x_{k+1} = f^n(x_k)$, and can generate an independent uniformly distributed chaotic key stream $\{s_i\}_0^\infty$ by the following process.

(1) *If $a > 0$, the chaotic attractor domain $[0,a]$ is partitioned into $N = 2^n$ subdomains $\tau_i = [t_i, t_{i+1})$, where $t_i = h(i/N)$, $i = 0, 1, \ldots, N-1$.*

(2) *If $a < 0$, the chaotic attractor domain $[a,0]$ is partitioned into $N = 2^n$ subdomains $\tau_i = [t_i, t_{i+1})$, where $t_i = h((N-i)/N)$, $i = 0, 1, \ldots, N-1$.*

(3) *Then, chaotic key stream $\{s_i\}_0^\infty$ is defined as:*

if $x_k \in \tau_i$, then $s_k = i$.

Proof. (1) *$f(x)$ Is Surjective*

When $ma = -4$, $f(x_k) = mx_k^2 + 4x_k = (-4/a)x_k^2 + 4x_k$.

If $a > 0$, it can be concluded that when $x_k \in [0,a]$, $f(x_k) \in [0,a]$.

If $a < 0$, it can be concluded that when $x_k \in [a,0]$, $f(x_k) \in [a,0]$.

Thus, $f(x)$ is surjective in its definition domain $[\min\{0,a\}, \max\{0,a\}]$.

(2) *Property of Topological Conjugation*

If f and g are topologically conjugated via h, then, according to Definition 2.1,

$$h^{-1} \circ f \circ h(x_k) = g(x_k), \quad \text{that is,} \ f \circ h(x_k) = h \circ g(x_k). \tag{2.6}$$

For Tent Map (2.3) and transformer (2.5),

$$\begin{aligned} h \circ g(x_k) &= \begin{cases} a\sin^2\dfrac{\pi 2x_k}{2} = a\sin^2\pi x_k, & 0 \leq x_k \leq \dfrac{1}{2} \\ a\sin^2\dfrac{\pi(2-2x_k)}{2} = a\sin^2(\pi - \pi x_k) = a\sin^2\pi x_k, & \dfrac{1}{2} \leq x_k \leq 1 \end{cases} \\ &= a\sin^2\pi x_k, \quad 0 \leq x \leq 1 \\ &= h(2x_k). \end{aligned} \tag{2.7}$$

When $ma = -4$, for map (2.4),

$$f(x_k) = \frac{-4}{a}x_k^2 + 4x_k = \frac{4}{a}x_k(a - x_k). \tag{2.8}$$

Hence,

$$\begin{aligned} f \circ h(x_k) &= \frac{4}{a} \cdot a\sin^2\frac{\pi x_k}{2}\left(a - a\sin^2\frac{\pi x_k}{2}\right) \\ &= 4a\sin^2\frac{\pi x_k}{2} \cdot \cos^2\frac{\pi x_k}{2} \\ &= a\left(2\sin\frac{\pi x_k}{2} \cdot \cos\frac{\pi x_k}{2}\right)^2 \\ &= a\sin^2\pi x_k. \end{aligned} \tag{2.9}$$

Thus, $f \circ h(x_k) = h \circ g(x_k)$.

Hence, f and g are topologically conjugated via h.

(3) *$f(x_k)$ Is Chaotic*

To assure the key stream $\{s_i\}_0^\infty$ produced by $f(x_k)$ is chaotic pseudorandom number with the potential characters proposed in paragraph 3 in Section 1, we prove the $f(x_k)$ is chaotic now.

As the reference [18–20] proposed, the Lyapunov exponents of corresponding orbits of two conjugated interval maps are the same. According to the computing method of Lyapunov exponent

$$\lambda(g,x) = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln\left|g'(x_i)\right|, \tag{2.10}$$

if $\lambda(g,x)$ is the Lyapunov exponent of the orbit of g through x, $\lambda(f,y)$ is the Lyapunov exponent of the orbit of f through $y = h(x)$, and $f \circ h(x_k) = h \circ g(x_k)$ is the conjugation, then $\lambda(g,x) = \lambda(f,y)$ [18]. And the largest $\lambda(g,x)$ with respect to changes of δx_0 is independent of x_0 [20].

More precisely, for the map (2.4) $f(y_k) = my_k^2 + 4y_k$ established by Theorem 2.4, Tent Map defined by (2.3), and $y_k = h(x_k) = a\sin^2(\pi x_k/2)$ defined by (2.5), we have $f \circ h(x_k) = h \circ g(x_k)$, and $f'(h(x_k)) \cdot h'(x_k) = h'(g(x_k)) \cdot g'(x_k)$, that is, $f'(y_k) \cdot h'(x_k) = h'(g(x_k)) \cdot g'(x_k)$, thus,

$$\left|f'(y_k)\right| = \left|\frac{h'(g(x_k))}{h'(x_k)}\right| \cdot \left|g'(x_k)\right| = \left|\frac{(\pi a/2)\sin(2\pi x_k)}{(\pi a/2)\sin(\pi x_k)}\right| \cdot \left|g'(x_k)\right| = |2\cos(\pi x_k)| \cdot \left|g'(x_k)\right|. \tag{2.11}$$

Also, for x_k in Tent Map, we have $\cos(\pi x_k) = \cos(\pi 2x_{k-1})$, then

$$\begin{aligned}
\lambda(f,y) &= \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln\left|f'(y_i)\right| = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln\left(|2\cos(\pi x_k)|\cdot\left|g'(x_k)\right|\right)\\
&= \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln(|2\cos(\pi x_k)|) + \lambda(g,x)\\
&= \lim_{n\to\infty}\frac{1}{n}\ln(|2\cos(\pi x_1)|\cdot|2\cos(\pi x_2)|\cdots|2\cos(\pi x_n)|) + \lambda(g,x)\\
&= \lim_{n\to\infty}\frac{1}{n}\ln\left(\frac{|\sin(\pi x_1)||2\cos(\pi x_1)|\cdot|2\cos(\pi x_2)|\cdots|2\cos(\pi x_n)|}{|\sin(\pi x_1)|}\right) + \lambda(g,x)\\
&= \lim_{n\to\infty}\frac{1}{n}\ln\left(\frac{|\sin(\pi x_1)||2\cos(\pi x_1)|\cdot|2\cos(\pi 2x_1)|\cdots|2\cos(\pi 2^n x_1)|}{|\sin(\pi x_1)|}\right) + \lambda(g,x)\\
&= \lim_{n\to\infty}\frac{1}{n}\ln\left(\frac{|\sin(\pi 2x_1)|\cdot|2\cos(\pi 2x_1)|\cdots|2\cos(\pi 2^n x_1)|}{|\sin(\pi x_1)|}\right) + \lambda(g,x)\\
&= \lim_{n\to\infty}\frac{1}{n}\ln\frac{|\sin(\pi 2^n x_1)|}{|\sin(\pi x_1)|} + \lambda(g,x)\\
&= \lim_{n\to\infty}\frac{1}{n}\ln|\sin(\pi 2^n x_1)| - \lim_{n\to\infty}\frac{1}{n}\ln|\sin(\pi x_1)| + \lambda(g,x)\\
&\leq \lim_{n\to\infty}\frac{1}{n}\ln n - 0 + \lambda(g,x) = \lambda(g,x) = \ln 2.
\end{aligned} \tag{2.12}$$

Hence, the largest Lyapunov exponent of $f(x)$ is $\ln 2$, and the map (2.4) is a chaotic system.

(4) *Chaotic Key Stream Is Uniformly Distributed*

From Lemma 2.3, the probability density function of f is

$$\rho_f = \rho_g\left(h^{-1}(x)\right)\left|\frac{dh^{-1}(x)}{dx}\right|. \tag{2.13}$$

Therefore, the probability of f in the domain $[t_i, t_{i+1})$ is

$$\begin{aligned}
\int_{t_i}^{t_{i+1}}\frac{dh^{-1}(x)}{dx}dx &= \int_{h(i/N)}^{h((i+1)/N)} dh^{-1}(x) = h^{-1}(x)\Big|_{h(i/N)}^{h((i+1)/N)}\\
&= h^{-1}\left(h\left(\frac{i+1}{N}\right)\right) - h^{-1}\left(h\left(\frac{i}{N}\right)\right)\\
&= \frac{i+1}{N} - \frac{i}{N} = \frac{1}{N}.
\end{aligned} \tag{2.14}$$

Thus, the value of chaos has the same probability in each domain, and, hence, chaotic key stream is uniformly distributed.

(5) *s_k Is Independent of s_{k+1} (Property of Independence)*

In this part, we will show that the value of s_{k+1} depends on the subdomains $\tau_i^j = [t_j^i, t_{j+1}^i)$, $j = 0, 1, \ldots, N-1$, $t_j^i = h((1/N)(i + j/N))$, where x_k is uniformly distributed according to the proof (4), and is independent of the τ_i to which x_k belongs.

For simplicity, we will only consider the condition $a > 0$. According to Definition 2.1, Lemma 2.2, and the sampling way $x_{k+1} = f^n(x_k)$, we get that, for $\theta \in [0,1]$, $x_k = h(\theta) = a\sin^2(\pi\theta/2)$ is increasing and has a one-to-one correspondence with θ, and $x_k \in \tau_j^i \Leftrightarrow \theta \in [(1/N)(i + j/N), (1/N)(i + (j+1)/N))$, then $x_{k+1} = h(2^n\theta) = a\sin^2(\pi 2^n\theta/2) \in h([i + j/N, i + (j+1)/N))$. For h is an even function with period 2, then

$$x_{k+1} \in h\left(\left[i + \frac{j}{N}, i + \frac{j+1}{N}\right)\right) = \begin{cases} \left[h\left(\dfrac{j}{N}\right), h\left(\dfrac{j+1}{N}\right)\right], & i \text{ is even} \\ \left[h\left(\dfrac{N-j-1}{N}\right), h\left(\dfrac{N-j}{N}\right)\right], & i \text{ is odd.} \end{cases} \tag{2.15}$$

Thus, when $s_k = i$,

$$s_{k+1} = \begin{cases} j, & i \text{ is even} \\ N - j - 1, & i \text{ is odd,} \end{cases} \tag{2.16}$$

that is, s_{k+1} is independent of s_k.

Considering (1) to (5), the theorem proposes a method to establish a class of topologically conjugated maps of Tent Map and can generate independently and uniformly distributed chaotic key stream. □

3. Examples of the Theorem 2.4

This section consists of the illustration of the deduction in [14], which is an example of the proposed theorem. To illustrate the effectiveness and feasibility of the proposed theorem, another example is provided to verify the chaotic property, independently and uniformly distributed property, and randomness of key streams. Due to the differences between theoretical values and calculated ones of a chaotic Logistic Map proposed in [21], all the examples are run with MATLAB (R2011a, v7.12) codes on the Window XP (32-bit) or Win7 (32-bit), and all the results are rounded into 4 digits after the decimal point.

Example 3.1. In Theorem 2.4, when $a = 1$, $m = -4$,

$$f(x_k) = -4x_k^2 + 4x_k = 4x_k(1 - x_k). \tag{3.1}$$

This map is the typical Logistic Map $f(x) = ux(1-x)$, when $u = 4$. It is used in [14] for the generation of key stream. According to Theorem 2.4, when $m = -4$, the $h(x) = \sin^2(\pi x_k/2)$, then the proof of Deduction 1 in [14] can be considered as an example of the theorem proposed in this paper.

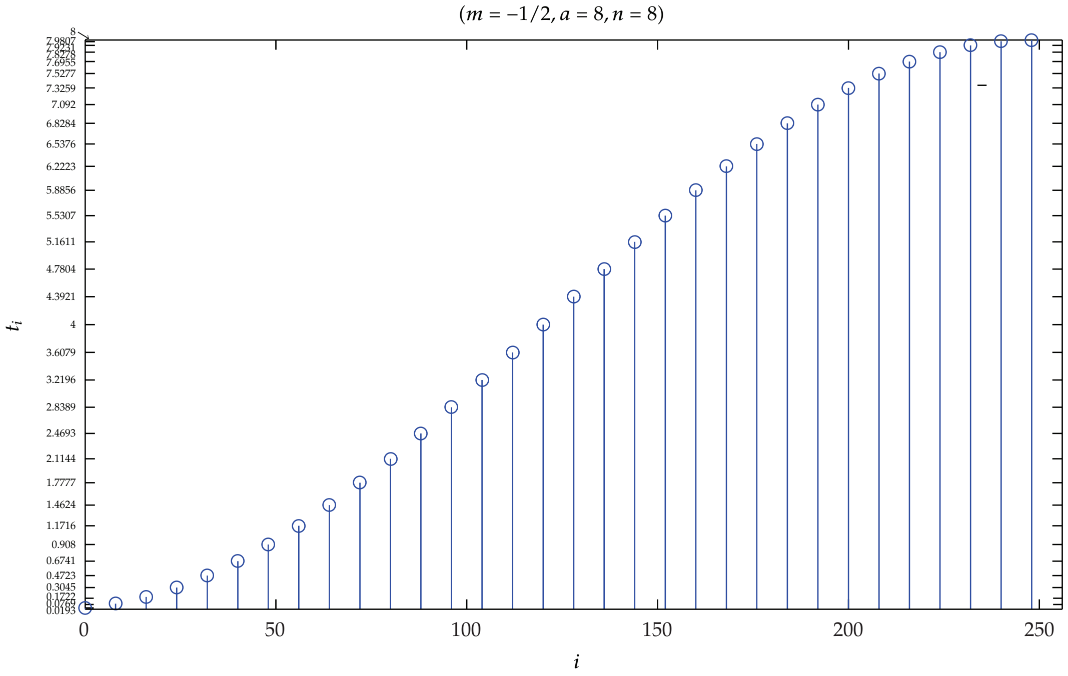


Figure 1: Partition of the attractor domain.

Example 3.2. In Theorem 2.4, we choose $a = 8$, $m = -1/2$, and another chaotic map is obtained as follows:

$$f(x_k) = -\frac{1}{2}x_k^2 + 4x_k, \tag{3.2}$$

and the transformer is

$$h(x_k) = 8\sin^2\frac{\pi x_k}{2}. \tag{3.3}$$

We choose $n = 8$ and divide the domain $[0, a] = [0, 8]$ into $2^n = 256$ intervals, each intervals' beginning pot and ending pot is shown in Figure 1. Not similar to the Tent Map, the partition of the attractor domain for i.i.d key stream generation is symmetric and is not uniform equal.

(1) *Chaotic Property of Map* (3.2)

For map (3.2), we set the initial condition $x_0 = 0.2323$, and the results of 1,000 iterations are shown in Figure 2. It is observed that the values are nonperiodic and are distributed in almost the entire domain.

(2) *Independently and Uniformly Distributed Property of* $\{s_i\}_0^\infty$

(a) χ^2 *Test* [22]

For the chaotic map (3.2) established by Theorem 2.4, we choose $x_0 = 0.2323$ and sampling step $n = 8$. After first 5,000 iteration abandoned, we get the 8-phase key stream $\{s_i\}_0^M$, where M is the lengths of sequence.

Table 1: Results of uniform distribution of key stream $\{s_i\}_0^M$ by map (3.2).

x_0	M	Threshold	χ^2	Result
0.2323	100,000	293.2478	281.9430	Pass
	200,000	293.2478	232.4326	Pass
	300,000	293.2478	239.8327	Pass
	400,000	293.2478	246.4038	Pass
	500,000	293.2478	246.6816	Pass

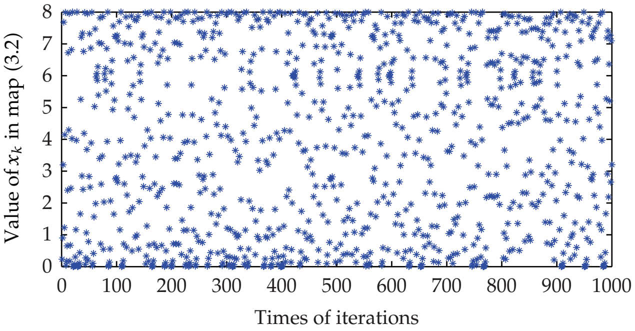


Figure 2: 1,000 iterations of map (3.2).

We set significance level $\alpha = 0.05$, then for M more than 100000, we get the same threshold $\chi^2_\alpha(M) = 293.2478$, and the results of χ^2 test are shown in Table 1, where all the results pass the test successfully.

Then we choose 100 random x_0 and set M as 20,000 to do χ^2 test. From the results in Figure 3, it can be observed that most of the tests passed and only 3 tests did not pass. As indicated in [12], the choice of initial value has an important impact on the statistical property of the chaotic system. Therefore, we can conclude that the key stream generated from Theorem 2.4 is uniformly distributed under the appropriate initial value.

(b) Approximate Entropy Analysis of $\{s_i\}_0^\infty$

For the chaotic map (3.2) established by Theorem 2.4, we choose $x_0 = 0.2323$ and sampling step $n = 8$. After first 5,000 iteration abandoned, we get the 8-phase key stream $\{s_i\}_0^M$, where M is the lengths of sequence.

According to the algorithm of approximate entropy in [23], we choose length of compared run lcr = 2, filtering level $r = 0.25\,\mathrm{SD}$, where SD is the standard deviation of $\{s_i\}_0^M$. For different M, we compute the approximate entropy of $\{s_i\}_0^M$ as shown in Table 2, where all the approximate entropies are close to the largest approximate entropy $\ln 8 = 2.0794$ for 8-ary key stream, which is inferred in [24] and follows Theorem 2 in [23].

Then we choose 100 random x_0 and set M as 6,000 with the same lcr = 2 and $r = 0.25\,\mathrm{SD}$ to compute the approximate entropy. From the results in Figure 4, it can be observed that the mean approximate entropy of $\{s_i\}_0^M$ is close to the maximum approximate entropy $\ln 8 = 2.0794$ which shows that the sequence produced by Theorem 2.4 has a certain complex degree.

(3) *Randomness Test of Key Streams* $\{s_i\}_0^\infty$

In this part, we change $\{s_i\}_0^\infty$ into binary sequences to carry out the test of NIST SP800-22 (April 2010), whose 15 tests depict the deviations of a binary sequence from

Table 2: Approximate entropy analysis of $\{s_i\}_0^M$ with different M.

lcr	r	x_0	M	Approximate entropy
2	0.25 SD	0.2323	3,000	2.0370
			4,000	2.0291
			5,000	2.0204
			6,000	2.0108
			7,000	2.0035
			8,000	2.0009
			9,000	1.9981

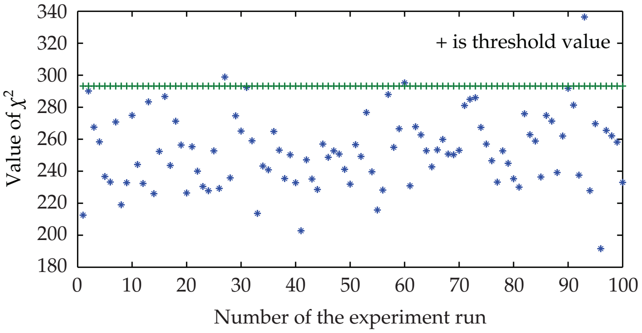


Figure 3: Result of χ^2 tests with 100 random number x_1.

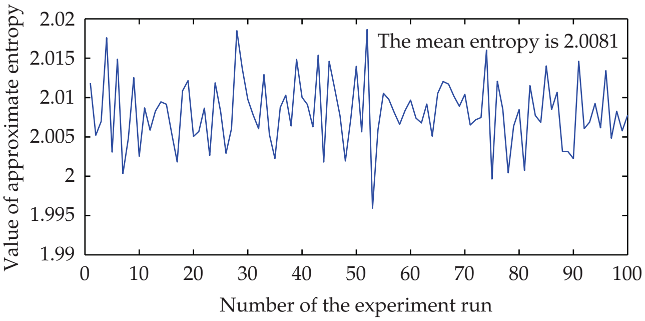


Figure 4: Result of approximate entropy with 100 random number x_1.

randomness [25]. P value, as the probability against the null hypothesis, represents the degree of randomness of the tested sequence. When we choose significance level $\alpha = 0.01$, if the value is bigger than $\alpha = 0.01$, it demonstrates that the sequence passes the test and could be considered as random. And the bigger the value is, the more random the sequences are.

First we use the chaotic map (3.2) established by Theorem 2.4 and choose $x_0 = 0.2323$, sampling step $n = 8$. After first 5,000 iteration abandoned, we get the 8-phase key stream $\{s_i\}_0^M$, where M is the lengths of sequence and $M = 125000$. Then we test the binary sequences $\{b_i\}_0^{1000000}$, which is changed from 8-phase sequence $\{s_i\}_0^M$, with NIST SP800-22. The results are shown in Table 3, implying that the key streams produced by theorem can satisfy the random requirements in NIST SP800-22.

Table 3: SP800-22 test's results.

Test	P value	Results
Frequency (monobit) test	0.4156	Random
Frequency test within a block	0.7311	Random
Runs test	0.5957	Random
Test for the longest run of ones in a block	0.7238	Random
Binary matrix rank test	0.9087	Random
Discrete fourier transform test	0.4573	Random
Nonoverlapping template matching test	0.4903 (mean)	Random
Overlapping template matching test	0.0173	Random
Maurer's "universal statistical" test	0.8827	Random
Linear complexity test	0.6231	Random
Serial test	0.7478 (mean)	Random
Approximate entropy test	0.0921	Random
Cumulative sums test	0.5617 (mean)	Random
Random excursions test	0.2387 (mean)	Random
Random excursions variant test	0.4487 (mean)	Random

Table 4: Mean P value and the passing ratio in SP800-22 tests with 100 random x_0.

Test	Mean P value	Passing ratio	Results
Frequency (monobit) test	0.4750	0.9900	Success
Frequency test within a block	0.8343	1.0000	Success
Runs test	0.8343	0.9900	Success
Test for the longest run of ones in a block	0.5749	1.0000	Success
Binary matrix rank test	0.0376	1.0000	Success
Discrete fourier transform test	0.2133	0.9800	Success
Nonoverlapping template matching test	0.4871	0.9907	Success
Overlapping template matching test	0.1719	0.9800	Success
Maurer's "universal statistical" test	0.4750	0.9900	Success
Linear complexity test	0.4944	0.9700	Success
Serial test	0.2739	1.0000	Success
Approximate entropy test	0.4944	0.9800	Success
Cumulative sums test	0.7488	0.9900	Success
Random excursions test	0.3408	0.9871	Success
Random excursions variant test	0.3988	0.9837	Success

Then we choose 100 random x_0 and set $M = 125000$ to do SP800-22 test, and Table 4 lists the mean P value and the passing ratio. For the significance level α set as 0.01, it means that 99% of test samples pass the tests if the random numbers are truly random. The acceptance region of the passing ratio is given by $[p-3\sqrt{p(1-p)/l}, p+3\sqrt{p(1-p)/l}]$, where l represents the number of the samples tested and $p = 1 - \alpha$ is the probability of passing each test [26]. For $l = 100$ and $p = 0.99$, we obtain the confidence interval $[0.9602, 1.0198]$, that is, $[0.9602, 1]$. From Table 4, we can get that the computed passing ratio for each test lies inside the confidence interval.

4. Conclusion

In this paper, we propose a new theorem for a class of topologically conjugated maps of Tent Map to generate independently and uniformly distributed key streams. Two examples are provided to validate that the key stream generated by the proposed theorem is theoretically and experimentally provedto be independently and uniformly distributed. We also conducted experiments for testing the randomness of these key streams, and all the key streams passed the NIST SP800-22 test. In future, this theorem could be applied to information security, numerical simulation, and other fields.

References

[1] L. Zhao, X. Liao, D. Xiao, T. Xiang, Q. Zhou, and S. Duan, "True random number generation from mobile telephone photo based on chaotic cryptography," *Chaos, Solitons and Fractals*, vol. 42, no. 3, pp. 1692–1699, 2009.

[2] Y. Hu, X. Liao, K. W. Wong, and Q. Zhou, "A true random number generator based on mouse movement and chaotic cryptography," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2286–2293, 2009.

[3] W. Xingyuan, Q. Xue, and T. Lin, "A novel true random number generator based on mouse movement and a one-dimensional chaotic map," *Mathematical Problems in Engineering*, vol. 2012, Article ID 931802, 9 pages, 2012.

[4] J. A. González and R. Pino, "Random number generator based on unpredictable chaotic functions," *Computer Physics Communications*, vol. 120, no. 2, pp. 109–114, 1999.

[5] L. Kocarev, G. Jakimoski, and Z. Tasev, "Chaos and pseudo-randomness," *Chaos Control, LNCIS*, vol. 292, pp. 682–685, 2003.

[6] A. Lasota M and M. Mackey, *Chaos, Fractals and Noise*, Springer, New York, NY, USA, 1994.

[7] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[8] F. James, "Chaos and randomness," *Chaos, Solitons & Fractals*, vol. 6, pp. 221–226, 1995.

[9] G. Jakimoski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," *IEEE Transactions on Circuits and Systems I*, vol. 48, no. 2, pp. 163–169, 2001.

[10] T. Stojanovski and L. Kocarev, "Chaos-based random number generators—part I: analysis," *IEEE Transactions on Circuits and Systems I*, vol. 48, no. 3, pp. 281–288, 2001.

[11] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators—part II: practical realization," *IEEE Transactions on Circuits and Systems I*, vol. 48, no. 3, pp. 382–385, 2001.

[12] A. Luca, A. Vlad, B. Badea, and M. Frunzete, "A study on statistical independence in the tent map," in *Proceedings of the International Symposium on Signals, Circuits and Systems (ISSCS '09)*, pp. 1–4, Iasi, Romania, July 2009.

[13] A. Luca, A. Ilyas, and A. Vlad, "Generating random binary sequences using tent map," in *Proceedings of the International Symposium on Signals, Circuits and Systems (ISSCS '11)*, pp. 81–84, Iasi, Romania, 2011.

[14] P. C. Wei, W. Zhang, and H. Q. Yang, "An image encryption algorithm based on coupled chaotic map," *Computer Science*, vol. 33, no. 11, pp. 237–255, 2006.

[15] H. P. Hu, S. H. Liu, Z. X. Wang, and X. G. Wu, "Method for generating chaotic key stream," *Chinese Journal of Computers*, vol. 27, no. 3, pp. 408–412, 2004.

[16] A. Luca and A. Vlad, "Generating identically and independently distributed samples starting from chaotic signals," in *Proceedings of the International Symposium on Signals, Circuits and Systems (ISSCS '05)*, pp. 227–230, Iasi, Romania, July 2005.

[17] B. L. Hao, *Starting with Parabola: An Introduction to Chaotic Dynamics*, Shanghai Scientific and Technological Education Publishing House, Shanghai, China, 1993.

[18] O. Knill, "Lyapunov exponent," 2005, http://www.math.harvard.edu/archive/118r_spring_05/handouts/Lyapunov.pdf.

[19] X. B. Liu, D. A. Zhao, and Z. Y. Zhu, "Analysis of security of chaotic sequence," *Journal of Jiangsu University of Science and Technology*, vol. 120, no. 14, pp. 51–54, 2006.

[20] W. H. Steeb, C. Villet, Y. Hardy, and R. Stoop, "Problems and solutions in chaos and fractals," http://issc.uj.ac.za/downloads/problems/ChaosFractals.pdf.

[21] S. C. Phatak and S. S. Rao, "Logistic map: a possible random-number generator," *Physical Review E*, vol. 51, no. 4, pp. 3670–3678, 1995.

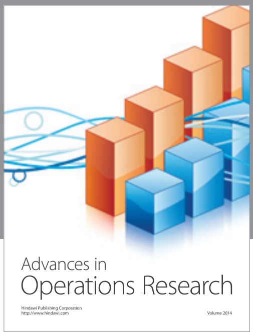
[22] M. S. Nikulin, “Chi-squared test for normality,” in *Proceedings of the International Vilnius Conference on Probability Theory and Mathematical Statistics*, vol. 2, pp. 119–122, 1973.

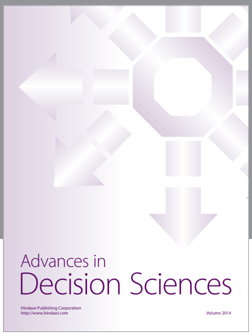
[23] S. M. Pincus, “Approximate entropy as a measure of system complexity,” *Proceedings of the National Academy of Sciences of the United States of America*, vol. 88, no. 6, pp. 2297–2301, 1991.

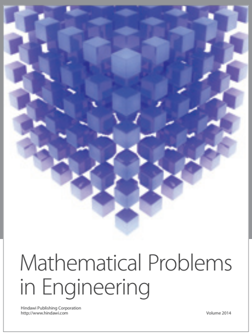
[24] A. L. Rukhin, “Approximate entropy for testing randomness,” *Journal of Applied Probability*, vol. 37, no. 1, pp. 88–100, 2000.

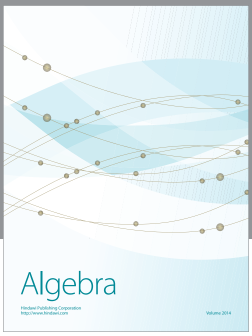
[25] NIST, “A statistical test suite for random and pseudo-random number generators for cryptographic applications,” 2010, http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

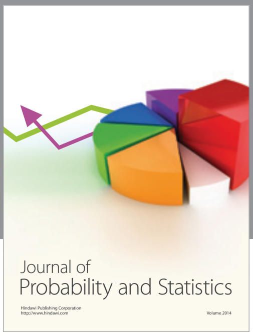
[26] D. A. Cristina, B. Radu, and R. Ciprian, “A new pseudorandom bit generator using compounded chaotic tent maps,” in *Proceedings of the 9th International Conference on Communications (COMM '12)*, pp. 339–342, 2012.


Advances in
Operations Research

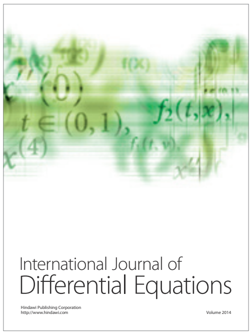

Advances in
Decision Sciences

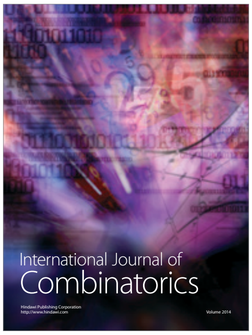

Mathematical Problems
in Engineering

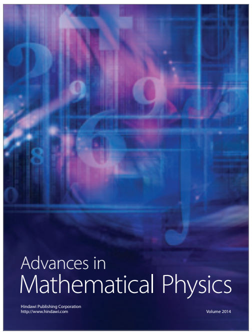

Algebra

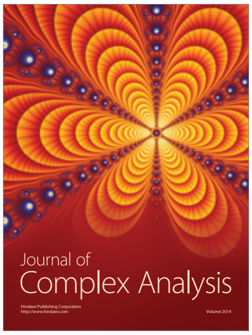

Journal of
Probability and Statistics

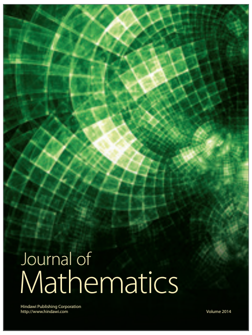
The Scientific
World Journal

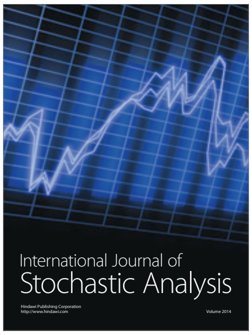

International Journal of
Differential Equations

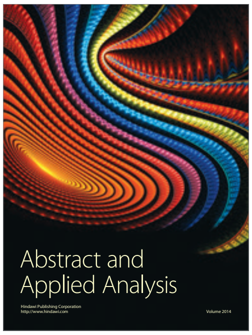

International Journal of
Combinatorics

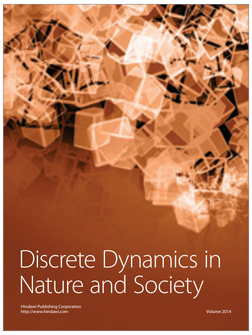

Advances in
Mathematical Physics

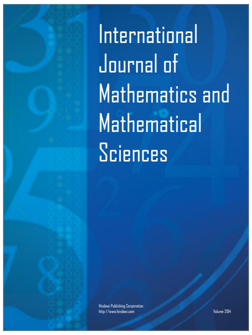

Journal of
Complex Analysis


Journal of
Mathematics


International Journal of
Stochastic Analysis

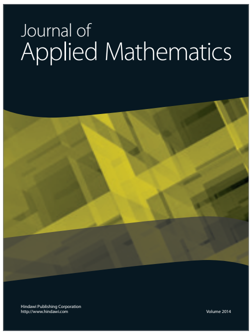

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


Journal of
Applied Mathematics

Journal of
Optimization