A pseudorandom bit generator based on arctangent function

Qi Wu

Department of E-Commerce, Jiangxi University of Finance & Economics, Nanchang, Jiangxi, 330013, China
1200600833@jxufe.edu.cn

Abstract. In this paper, in addition to translation & scale (already adopted before), we employ another elementary transformation, i.e. fold, to acquire a variant of Arctangent Function. Both Bifurcation Diagram & Lyapunov Exponent Spectrum indicate that the new mapping owns excellent chaotic properties. Afterwards, a pseudorandom bit generator is devised based on it. Pseudorandom tests illustrate that the mapping is the 3rd best one so far. The results show great application prospect.

1. Introduction

In [1], it is concluded that unimodal mappings usually possess chaotic properties. However, [1] does not consider what kind of unimodal mappings could possess chaotic properties. After many years of experiments [2-16], we have experienced a number of failures and obtained only a few successes [5,6,12,13,14,16].

In our previous papers [14,16], we only applied translation & scale on elementary functions to form unimodal mappings. If we refuse to widen our eyes, we demand the original functions to be ascendant on the left segment and descendant on the right segment, as neither translation nor scale could change the monotonicity of functions.

In this paper, we take into account another elementary transformation, i.e. fold, to obtain unimodal mappings. Via fold, we will not confine our concern in functions which are first ascendant then descendant. Functions which are constantly ascendant or descendant could be taken into account, as after partly folded, they could easily meet our requirement.

The upcoming parts are as follows: Section 2 introduces a chaotic mapping based on transformed arctangent function (via fold, translation & scale). Section 3 aims to apply it to the construction of Pseudorandom bit Generator (abbr. PRBG). Section 4 concludes.

2. A chaotic mapping based on transformed arctangent function

It is known that, Arctangent function:

\[ A(x) = \arctan x \]  \hspace{1cm} (1)

goes through point \((0,0)\) and is centrosymmetric on it.

Next, let’s fold its right half vertically, to obtain a new function:

\[ A_2(x) = \begin{cases} 
\arctan x, & x \leq 0 \\
-\arctan x, & x > 0 
\end{cases} \]  \hspace{1cm} (2)

It is easy to see that \( A_2 \) is axisymmetric on \( y \) axis.

Then, let’s translate the peak of \( A_2 \) (point \((0,0)\)) to point \((0.5,1)\), to acquire a new function:
\[ A_3(x) = \begin{cases} \arctan(x - 0.5) + 1, & x \leq 0.5 \\ -\arctan(x - 0.5) + 1, & x > 0.5 \end{cases} \]  

(3)

Afterwards, let's apply scale to \( A_3 \):

\[ b[A_3(x) - 1] = \begin{cases} \arctan[a(x - 0.5)], & x \leq 0.5 \\ -\arctan[a(x - 0.5)], & x > 0.5 \end{cases} \]  

(4)

Next, we slightly change the form of equation (4):

\[ A_4(x) = \begin{cases} b \arctan[a(x - 0.5)] + 1, & x \leq 0.5 \\ -b \arctan[a(x - 0.5)] + 1, & x > 0.5 \end{cases} \]  

(5)

Note that \( b \) in equation (4) is different from \( b \) in equation (5). Then, we demand that the left segment of \( A_4 \) goes through point \((0,0)\) and the right segment of \( A_4 \) goes through point \((1,0)\). So, we have:

\[-b \arctan(0.5a) + 1 = 0, \]  

(6)

\[ b = \frac{1}{\arctan(0.5a)}. \]  

(7)

In conclusion, the variant of Arctangent function equation (5) obtained in this paper possesses only one free parameter \( a \). Once \( a \) is fixed in \((-\infty, +\infty)\) (In terms of our experiments, most of good values for \( a \) lie in interval \([-0.5, 0.5]\)), \( b \) is settled accordingly via equation (7). Thus, the entire mapping equation (5) is fixed.

For convenience, henceforth, we name the new mapping equation (5) **Arctangent Function’s Variant Chaotic Mapping** (often abbreviated as **AFVCM**).

Next, let’s analyze its chaotic properties.

For AFVCM, set \( x_0=0.1 \), let \( a \) go from -0.5 to 0.5 with step 0.00001. For the 100001 parameters, iterate the system 500 times respectively, filtering the first 200 times, draw the \( x \) value for the last 300 times as shown in figure 1.

![Figure 1. Bifurcation diagram.](image)

From figure 1 it could be seen that, for the aforementioned initial values and parameters, AFVCM doesn’t own any obvious periodic area and is quite suitable for PRBG.

Set \( x_0=0.1 \), let \( a \) go from -0.5 to 0.5 with step 0.00001. For the 100001 parameters, iterate the system 2000 times, filtering the first 1000 times, calculate the Lyapunov exponent from the last 1000 times as shown in figure 2.
From figure 2 it could be seen that, for the initial values and parameters mentioned above, the Lyapunov exponent of AFVCM is always positive, i.e. the system always dwells in chaotic area. Therefore, it fits PRBG wonderfully.

3. A PRBG based on AFVCM
In this paper we devise PRBG the same as in [13]. Given \(x_0, a\), AFVCM acquires a new \(x_i\) after each iteration, compares it with 0.5 to emit a new bit:

\[
s_i = \begin{cases} 
0, & x_i < 0.5 \\
1, & x_i \geq 0.5 
\end{cases}
\]  

(8)

In [13], when \(c\) goes from -1000 to 0 with step 0.01, for the 100001 parameters, there are 60841 ones passing all the 5 pseudorandom tests. (i.e. about 60% parameters are strong, which is the champion of 1-Dimensional Discrete Chaotic Mapping (abbr. 1DDCM).) In [16], when \(a\) goes from -100 to -1.001 and 0.001 to 100 with step 0.001, for the 199000 parameters, there are 94612 ones passing the tests. (i.e. approximately 48% parameters are strong, which is the silver medalist of 1DDCM.) As to the PRBG in this paper, this result becomes 77545. (\(a\) goes from -0.5 to 0.5 with step 0.000005. i.e. about 39% parameters are strong, which is the copper medalist of 1DDCM. Although it is poorer than [13,16], it has already overwhelmed Logistic mapping & skew tent mapping, which are the most classic ones.)

Next, for \(x_0=0.1\), this paper tests 3 bit streams of length 50000 with \(a\) set to -0.05, 0.1, 0.3 respectively and acquires results under significance level 0.05. In this paper all the basic knowledge for tests is omitted. Readers interested in them could refer to [2-16].

Table 1-5 illustrate that, all the 3 bit streams have passed the 5 pseudorandom tests. As BM algorithm is too time-consuming, this paper sets the length of bit streams to 1000 while computing Table 6 with all the other conditions unchanged. It is obvious that all the 3 bit streams own excellent Linear Complexity (All are close to BSS.).

Table 1. Results of monobit test.

| \(a\)  | \(\chi^2\)  | Critical value |
|-------|-------------|----------------|
| -0.05 | 0.0013      |                |
| 0.1   | 0.4621      | 3.84           |
| 0.3   | 0.9857      |                |
Table 2. Results of serial test.

| a   | \(X^2\) | Critical value |
|-----|---------|----------------|
| -0.05 | 0.1818 |                |
| 0.1  | 0.8719 | 5.99           |
| 0.3  | 1.8594 |                |

Table 3. Results of poker test.

| a   | \(X^2(m=4)\) | Critical value |
|-----|--------------|----------------|
| -0.05 | 16.1370        |                |
| 0.1  | 10.8762       | 25             |
| 0.3  | 20.0922       |                |

Table 4. Results of runs test.

| a   | \(X^2\) | Critical value |
|-----|---------|----------------|
| -0.05 | 13.5644 |                |
| 0.1  | 12.7814 | 31.4           |
| 0.3  | 18.9612 |                |

Table 5. Results of auto-correlation test.

| a   | \(|X|(d=10000)\) | Critical value |
|-----|-----------------|----------------|
| -0.05 | 1.16             |                |
| 0.1  | 0.46            | 1.96           |
| 0.3  | 0.33             |                |

Table 6. Results of linear complexity.

| a   | Linear complexity | \(N/2\) |
|-----|-------------------|---------|
| -0.05 | 501              |         |
| 0.1  | 500              | 500     |
| 0.3  | 499              |         |

4. Conclusion
Based on Arctangent Function, after folding, translation and scale, we obtain a variant mapping with 1 free parameter. Both Bifurcation Diagram & Lyapunov Exponent Spectrum demonstrate that the new mapping possesses wonderful chaotic properties. Based on it, a PRBG is devised. Its strong cipher space is smaller compared to our best 2 results [13,16], but it has already overwhelmed Logistic mapping & skew tent mapping. All the statistical tests illustrate that, the bit streams generated own excellent pseudo randomness and superior linear complexity.

In the future, we will decide to test other 1DDCMs and try to exceed our best result.

Acknowledgments
This research is financially supported by the Science and Technology Project of Provincial Education Department of Jiangxi for Youth (GJJ180288). Thanks go to Shiqian Wu, Zhihong Guan and Meng Jia.
References

[1] Hao, B.L. (1993) Starting with Parabolas. Shanghai Science and Technology Education Press, Shanghai.

[2] Tan, Z.W., Wu, Q. (2008) Study of Linearly Cross-Coupled Chaotic Systems for a Random Bit Generator. In: International Conference on Computational Intelligence and Security. Suzhou.

[3] Tan, Z.W., Wu, Q. (2008) Study of Exponentially Cross-Coupled Chaotic Systems for a Random Bit Generator. In: International Symposium on Intelligent Information Technology Application. Shanghai. pp. 224-227.

[4] Wu, Q., Tan, Z.W., Wan, C.X. (2011) A Harmonically Coupled Chaotic System for a Pseudo-Random Bit Generator. Journal of Chinese Computer Systems, 32: 639-643.

[5] Wu, Q. (2015) A Chaos-based Hash Function. In: International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Xi’an.

[6] Wu, Q. (2016) A Quartic Chaotic Mapping. In: International Conference on Computer Science and Information Security. Nanjing.

[7] Wu, Q. (2016) Independent Variable Exclusively Coupled Chaotic Pseudorandom Bit Generator. Computer Engineering & Science, 38: 2197-2201.

[8] Wu, Q. (2016) An Independent Variable Exclusively Coupled Chaotic System for a Pseudorandom Bit Generator. In: International Conference on Industrial Informatics – Computing Technology, Intelligent Technology, Industrial Information Integration. Wuhan. pp. 341-344.

[9] Wu, Q. (2018) A Dependent Variable Harmonically Coupled Chaotic System for a Pseudorandom Bit Generator. In: International Conference on Smart Materials, Intelligent Manufacturing and Automation. Hangzhou.

[10] Wu, Q. (2018) A Dependent Variable Exclusively Coupled Chaotic System for a Pseudorandom Bit Generator. In: International Conference on Network and Information Systems for Computers. Wuhan.

[11] Wu, Q. (2018) A Pseudorandom Bit Generator based on a Dependent Variable Exclusively Coupled Chaotic System. In: International Conference on Intelligent Information Processing. Guilin. pp. 11-16.

[12] Wu, Q. (2019) Another Look at a Proposed Quartic Chaotic Mapping. In: International Symposium on Advances in Electrical, Electronics and Computer Engineering. Zhuhai.

[13] Wu, Q. (2019) Another Look at a Proposed Cubic Chaotic Mapping. In: International Symposium on Cyberspace Safety and Security. Guangzhou.

[14] Wu, Q. (2020) Piecewise Multi-Parameter Tangent/Cotangent Function and its Application in Chaotic Pseudorandom Bit Generator. In: International Conference on Energy, Power, Environment and Computer Application. Beijing.

[15] Wu, Q. (2020) An Independent Variable Swinging Coupled Chaotic System for a Pseudorandom Bit Generator. International Journal of Network Security, in press.

[16] Wu, Q. (2020) A Pseudorandom Bit Generator based on Gaussian Function, unpublished.