# A pseudorandom bit generator based on hyperbolic cosine function

*Qi* Wu*

Department of E-Commerce, Jiangxi University of Finance & Economics, Nanchang, Jiangxi, 330013, China

**Abstract.** In the literature, little attention is paid to devising and analyzing novel one dimensional chaotic mappings. In our previous efforts, we have tried fold, translation & scale on arctangent function & sigmoid function respectively, which brings good results. In this paper, we do the same to obtain a variant of Hyperbolic Cosine Function. Both Bifurcation Diagram & Lyapunov Exponent Spectrum manifest that the new mapping possesses wonderful chaotic properties. Then, a pseudorandom bit generator is designed based on it. Pseudorandom tests demonstrate that the generator is much better than our previous ones. It owns great application prospect.

**Keywords:** Chaotic mapping, Hyperbolic cosine function, Pseudorandom bit generator.

## 1 Introduction

In [1], it is proposed that unimodal mappings usually own chaotic properties. However, [1] does not elaborate on what type of unimodal mappings could own chaotic properties. After many years of experiments [2-18], we have experienced a lot of failures and acquired only a few successes [5,6,12,13,14,16,17,18].

In our previous papers [17,18], in addition to translation & scale, we apply fold to elementary functions to obtain unimodal mappings. This approach has tremendously broadened our horizon. We will not command the original functions to be ascendant on the left segment and descendant on the right segment, as fold could change the monotonicity of functions. Functions which are constantly ascendant, such as Arctangent Function [17] & Sigmoid Function [18], work well after partly folded.

In this paper, we extend our approach to **Hyperbolic Cosine Function** and see what could be achieved.

The upcoming parts are as follows: Section II introduces a chaotic mapping based on transformed Hyperbolic Cosine Function (via fold, translation & scale). Section III manages to apply it to devising Pseudorandom bit Generator (abbr. **PRBG**). Section IV concludes.

* Corresponding author: wuqiocjzd@126.com

## 2 A chaotic mapping based on transformed hyperbolic cosine function

It is known that, Hyperbolic Cosine function:

$$C(x) = \cosh(x) \tag{1}$$

Goes through point (0,1) and is axisymmetric on *y* axis.

Next, let us fold it vertically, to acquire a new function:

$$C_2(x) = -\cosh(x). \tag{2}$$

It is easy to see that $C_2$ goes through point (0,-1) and is axisymmetric on *y* axis.

Then, let us translate the peak of $C_2$ (point (0,-1)) to point (0.5,1), to obtain a new function:

$$C_3(x) = -\cosh(x - 0.5) + 2. \tag{3}$$

Afterwards, let us apply scale to $C_3$:

$$b[C_3(x) - 1] = -\cosh[a(x - 0.5)] + 1. \tag{4}$$

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

$$C_4(x) = -bcosh[a(x - 0.5)] + b + 1. \tag{5}$$

Note that $b$ in equation (4) is different from $b$ in equation (5). Then, we demand that the left segment of $C_4$ goes through point (0,0) and the right segment of $C_4$ goes through point (1,0). So, we have:

$$-bcosh(0.5a) + b + 1 = 0, \tag{6}$$

$$b = \frac{1}{\cosh\left(\frac{a}{2}\right) - 1}. \tag{7}$$

In conclusion, the variant of Hyperbolic Cosine 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 (-1.5, 1.5).), $b$ is settled accordingly via equation (7). Thus, the entire mapping equation (5) is fixed.

For convenience, henceforth, we name the new mapping equation (5) **Hyperbolic Cosine Function's Variant Chaotic Mapping** (often abbreviated as **HCFVCM**).

Next, let us analyze its chaotic properties.

For HCFVCM, set $x_0$=0.1, let $a$ go from -1.49999 to 1.49999 with step 0.00001. For the 299999 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.

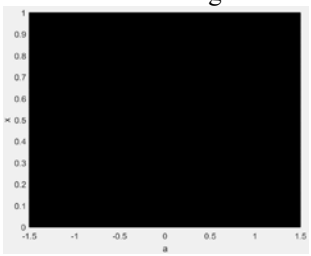


**Fig. 1.** Bifurcation diagram.

From figure 1 it could be seen that, for the aforementioned initial values and parameters, HCFVCM does not own any obvious periodic area and is quite suitable for PRBG.

Set $x_0$=0.1, let $a$ go from -1.49999 to 1.49999 with step 0.00001. For the 299999 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.

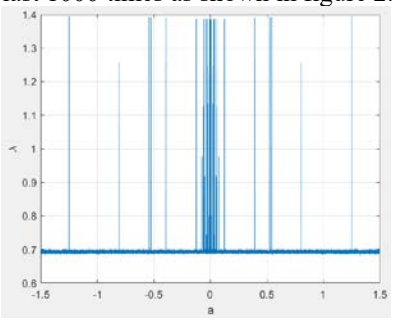


**Fig. 2.** Lyapunov exponent spectrum.

From figure 2 it could be seen that, for the initial values and parameters mentioned above, the Lyapunov exponent of HCFVCM is always positive, i.e. the system always dwells in chaotic area. Therefore, it fits PRBG wonderfully.

## 3 A PRBG based on HCFVCM

In this paper we devise PRBG the same as in [17,18]. Given $x_0$, $a$, HCFVCM acquires a new $x_i$ after each iteration, compares it with 0.5 to emit a new bit:

$$s_i = \begin{cases} 0, x_i < 0.5 \\ 1, x_i \geq 0.5 \end{cases}. \tag{8}$$

In [17], when $a$ goes from -0.5 to 0.5 with step 0.000005, for the 200001 parameters, there are 77545 ones passing all the 5 pseudorandom tests. (i.e. approximately 39% parameters are strong.) In [18], when $a$ goes from -1 to 1 with step 0.00001, for the 200001 parameters, there are 76794 ones passing the tests. (i.e. about 38% parameters are strong.) As to the PRBG in this paper, this result becomes **138381** when $a$ goes from -1.49999 to 1.49999 with step 0.00001. (i.e. about 46% parameters are strong, which outperforms [17] & [18].)

Next, for $x_0$=0.1, this paper tests 3 bitstreams of length 50000 with $a$ set to -0.9, 0.8, 1.1 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 [2-18].

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

**Table 1.** Results of monobit test.

| | | |
|---|---|---|
| $a$ | $X^2$ | Critical value |
| -0.9 | 1.5457 | 3.84 |
| 0.8 | 0.0051 | |
| 1.1 | 0.6771 | |

**Table 2.** Results of serial test.

| *a* | $X^2$ | Critical value |
|---|---|---|
| -0.9 | 1.9434 | 5.99 |
| 0.8 | 1.6988 | |
| 1.1 | 0.7076 | |

**Table 3.** Results of poker test.

| *a* | $X^2$(*m*=4) | Critical value |
|---|---|---|
| -0.9 | 12.1331 | 25 |
| 0.8 | 13.8611 | |
| 1.1 | 9.2864 | |

**Table 4.** Results of runs test.

| *a* | $X^2$ | Critical value |
|---|---|---|
| -0.9 | 26.4242 | 31.4 |
| 0.8 | 17.0138 | |
| 1.1 | 17.6583 | |

**Table 5.** Results of auto-correlation test.

| *a* | \|X\|(*d*=10000) | Critical value |
|---|---|---|
| -0.9 | 0.46 | 1.96 |
| 0.8 | 0.15 | |
| 1.1 | 1.41 | |

**Table 6.** Results of linear complexity.

| *a* | Linear complexity | *N*/2 |
|---|---|---|
| -0.9 | 500 | 500 |
| 0.8 | 501 | |
| 1.1 | 500 | |

## 4 Conclusion

Based on Hyperbolic Cosine 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 larger than our previous 2 results [17,18]. All the statistical tests illustrate that, the bitstreams generated own excellent pseudo randomness and superior linear complexity.

In the future, we decide to check other elementary functions and try to achieve even better results.

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: Shanghai Science and Technology Education Press)
2. Tan Z W and Wu Q 2008 *Proc. Int. Conf. on Computational Intelligence and Security (Suzhou)*
3. Tan Z W and Wu Q 2008 *Proc. Int. Symp. on Intelligent Information Technology Application (Shanghai)* p 224
4. Wu Q, Tan Z W and Wan C X 2011 A Harmonically Coupled Chaotic System for a Pseudo-Random Bit Generator *Journal of Chinese Computer Systems* vol 32 pp 639-643
5. Wu Q 2015 *Proc. Int. Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery (Xi'an)*
6. Wu Q 2016 *Proc. Int. Conf. on Computer Science and Information Security (Nanjing)*
7. Wu Q 2016 Independent Variable Exclusively Coupled Chaotic Pseudorandom Bit Generator. *Computer Engineering & Science* vol 38 pp 2197-2201
8. Wu Q 2016 *Proc. Int. Conf. on Industrial Informatics – Computing Technology, Intelligent Technology, Industrial Information Integration (Wuhan)* p 341
9. Wu Q 2018 *Proc. Int. Conf. on Smart Materials, Intelligent Manufacturing and Automation (Hangzhou)*
10. Wu Q 2018 *Proc. Int. Conf. on Network and Information Systems for Computers (Wuhan)*
11. Wu Q 2018 *Proc. Int. Conf. on Intelligent Information Processing (Guilin)* p 11
12. Wu Q 2019 *Proc. Int. Symp. on Advances in Electrical, Electronics and Computer Engineering (Zhuhai)*
13. Wu Q 2019 *Proc. Int. Symp. on Cyberspace Safety and Security (Guangzhou)*
14. Wu Q 2020 *Proc. Int. Conf. on Modeling, Simulation and Optimization Technologies and Applications (Beijing)*
15. Wu Q 2021 An Independent Variable Swinging Coupled Chaotic System for a Pseudorandom Bit Generator *International Journal of Network Security* vol 23 pp 774-778
16. Wu Q 2022 A Pseudorandom Bit Generator based on Gaussian Function, in press.
17. Wu Q 2021 *Proc. Int. Conf. on Computer Network Security and Software Engineering (Zhuhai)*
18. Wu Q 2021 *Proc. Int. Conf. on Information Communication and Software Engineering (Chengdu)*