A Dependent Variable Harmonically Coupled Chaotic System for a Pseudorandom bit Generator

Qi Wu

*Department o*Department of Computer Science & Technology, School of Information Technology, Jiangxi UniveJiangxi University of Finance & Economics, Nanchang, China

Abstract: Coupling is a common approach for constructing new chaotic systems. In this paper, we present a novel way of coupling, which is utilized to construct a new chaotic system. Afterwards, a pseudorandom bit generator is proposed based on it. Next, we employ five statistic tests to evaluate the pseudo randomness of generated sequences. Linear complexity and cipher space are analyzed at last. All the results demonstrate that the proposed generator possesses excellent properties.

1 INTRODUCTION

In 1949, Shannon put forward that cryptosystems should own two characteristics, confusion and diffusion (Shannon, 1949). Chaotic systems move so irregularly that patterns could hardly be recognized, which resembles confusion. Chaotic systems are extremely keen to parameters and initial values that minute variation in them will be amplified enormously, which resembles diffusion. Therefore, many efforts have been made to apply chaos to cryptology, one of which is designing pseudorandom bit generators (usually abbreviated as **PRBG**) based on chaotic systems (Qi, 2017; Hu, 2017; Wu, 2017).

Coupling is a common approach for constructing new chaotic systems. Ways of coupling are categorized into four classes by us (Wu, 2011), i.e. perturbation coupling (Liu, 2006; Bao, 2007; Yu, 2005; Ma, 2013), independent variable-dependent variable coupling (Wu, 2007), dependent variable coupling (Liu, 2007; Liu, 2008; Luo, 2012), and independent variable coupling (Tan, 2008a; Tan, 2008b; Wu, 2011; Wu, 2016a; Wu, 2016b). As to the aforementioned classes, the former two are deemed suitable for chaos control, while the latter two are deemed proper for chaos anti-control, which implies prospective for cryptographic applications.

Independent variable coupling has been vastly examined by us (Tan, 2008a; Tan, 2008b; Wu, 2011; Wu, 2016a; Wu, 2016b), whereas most of its dependent variable counterparts is left unconcerned, except dependent variable linearly coupling (Liu, 2007; Liu, 2008; Luo, 2012). Via our experiments, dependent variable coupling usually performs as wonderfully as independent variable coupling, and should be paid attention to.

In this paper, we propose a new kind of coupling, i.e. dependent variable harmonically coupling, then apply it to skew tent mapping to obtain a 2D discrete chaotic system. Afterwards, a PRBG is devised based on it. Statistical tests testify the generated sequences hold good pseudo randomness. At last, linear complexity and cipher space are calculated as well. All the experiments illustrate that the proposed PRBG is a wonderful candidate.

We organize the upcoming parts of this paper as follows. In Section 2, a chaotic system is constructed and analyzed. In Section 3, we devise a PRBG and analyze the pseudo randomness of generated sequences via five statistic tests. In Section 4, the linear complexity is computed. In Section 5, the cipher space is calculated. Section 6 concludes.

2 DEPENDENT VARIABLE HARMONICALLY COUPLED CHAOTIC SYSTEM

First, let's explain the difference between independent variable coupling and dependent variable coupling.

Given two skew tent mappings defined as:

$$x_{i+1} = f_\alpha(x_i) = \begin{cases} \dfrac{x_i}{\alpha} & x_i \in [0, \alpha] \\ \dfrac{1 - x_i}{1 - \alpha} & x_i \in (\alpha, 1] \end{cases}, \quad (1)$$

* *Corresponding author: wuqiocjzd@126.com*

$$y_{i+1} = f_\alpha(y_i) = \begin{cases} \dfrac{y_i}{\alpha} & y_i \in [0, \alpha] \\ \dfrac{1 - y_i}{1 - \alpha} & y_i \in (\alpha,1] \end{cases}, \quad (2)$$

importing a coupling function g, independent variable coupling applies g first and f next, i.e. the new chaotic system becomes

$$\begin{cases} x_{i+1} = f_\alpha(g_u(x_i, y_i)) \\ y_{i+1} = f_\alpha(g_u(y_i, x_i)) \end{cases}. \quad (3)$$

As to dependent variable coupling, it applies f first and g next, i.e. the new chaotic system becomes

$$\begin{cases} x_{i+1} = g_u(f_\alpha(x_i), f_\alpha(y_i)) \\ y_{i+1} = g_u(f_\alpha(y_i), f_\alpha(x_i)) \end{cases}. \quad (4)$$

In this paper, we adopt the same g as (Wu, 2011):

$$g_u(r, s) = \frac{1}{\dfrac{u}{r} + \dfrac{1 - u}{s}}, \quad (5)$$

i.e. it's the weighted harmonic average of its input. Thus, we call our new chaotic system (using Equation (4)) Dependent Variable Harmonically Coupled Chaotic System (abbreviated as **DVHCCS** hereafter). Next, let's analyse its chaotic properties.

Let $x_0 = 0.6$, $y_0 = 0.3$, $\alpha = 0.5$, u goes from 0 to 1 with step=0.001. For the 1001 parameters, iterate DVHCCS 500 times, filter the first 200 times, and depict the values of x for the last 300 times, as shown in Figure 1.

From the bifurcation graph, we can see the chaotic area of DVHCCS lies in $[0,0.3] \cup [0.7,1]$, where candidates for PRBG may dwell.

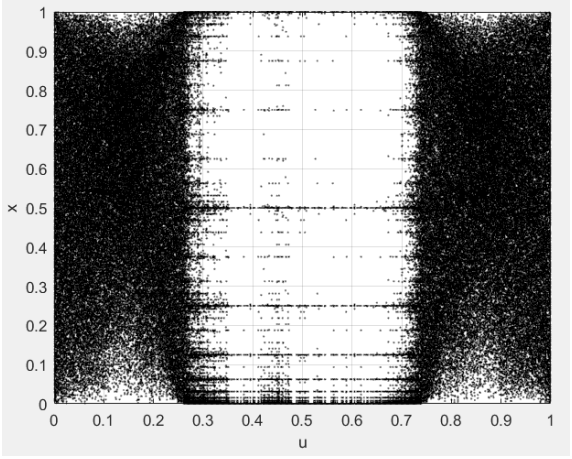

Figure 1: Bifurcation graph.

Next, recall the definition for Lyapunov exponent of 2D discrete dynamic system.

Given a 2D discrete dynamic system defined as:

$$\begin{cases} x_{i+1} = f_1(x_i, y_i) \\ y_{i+1} = f_2(x_i, y_i) \end{cases}, \quad (6)$$

its corresponding Jacobian matrix is

$$J_i = \begin{bmatrix} \dfrac{\partial f_1}{\partial x_i} & \dfrac{\partial f_1}{\partial y_i} \\ \dfrac{\partial f_2}{\partial x_i} & \dfrac{\partial f_2}{\partial y_i} \end{bmatrix}, \quad (7)$$

then the Lyapunov exponents for system (6) are

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln|\mu_i|, \quad (8)$$

where μ_i is the eigenvalue of J_i. J_i has 2 eigenvalues, so system (6) owns 2 Lyapunov exponents, obtained by calculating (8) respectively for each eigenvalue of J_i in every iterations.

Let $x_0 = 0.6$, $y_0 = 0.3$, $\alpha = 0.5$, u goes from 0 to 1 with step=0.0001. For the 10001 parameters, iterate DVHCCS 6000 times, filter the first 5000 times, and depict the Lyapunov exponents for the last 1000 times, as shown in Figure 2.

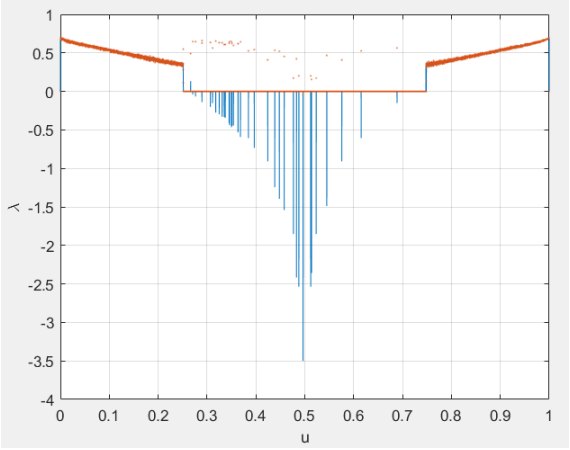

Figure 2: Lyapunov exponent graph.

In Figure 2, the two Lyapunov exponents are depicted with lines and points, respectively. It's known that a dynamic system lies in chaotic area iff its largest Lyapunov exponent is positive. Apparently, the majority of the chaotic area of IVECCS lies in $[0,0.25] \cup [0.75,1]$, where possibility for PRBG may exist.

3 A PROPOSED PRBG

Here, we design a PRBG based on DVHCCS following the framework of (Li, 2001).

Given x_0, y_0, α, u, after each iteration, emit a bit s_i via comparing x_i and y_i:

$$s_i = \begin{cases} 0, x_i < y_i \\ 1, x_i \geq y_i \end{cases}. \quad (9)$$

In (Wu, 2011), when both α and u go from 0 to 1 with step=0.0001, for the 100020001 pairs of parameters, 7638 $\alpha - u$ ones pass all 5 tests for pseudo randomness. As to DVHCCS, the result rises to 7735 pairs.

Next, we employ 5 statistic tests for pseudo randomness and illustrate the results of tests under level of significance 0.05 for 3 sequences of length 50000 generated when $x_0 = 0.49$, $y_0 = 0.55$, α and u set to (0.499,0.249), (0.502,0.248), (0.659,0.839) , respectively.

From Table 1 to 5, the test results for the 3 sequences are all less than the critical values, indicating the preferable pseudorandom properties of the generator.

Table 1: Results of monobit test.

α	u	χ^2	Critical value
0.499	0.249	0.0583	3.84
0.502	0.248	3.4611	
0.659	0.839	0.3920	

Table 2: Results of serial test.

α	u	χ^2	Critical value
0.499	0.249	2.8666	5.99
0.502	0.248	4.2375	
0.659	0.839	0.4158	

Table 3: Results of poker test.

α	u	$\chi^2(m = 4)$	Critical value
0.499	0.249	12.9088	25
0.502	0.248	10.1747	
0.659	0.839	23.5917	

Table 4: Results of runs test.

α	u	χ^2	Critical value
0.499	0.249	22.4607	31.4
0.502	0.248	24.4852	
0.659	0.839	30.2192	

Table 5: Results of auto-correlation test.

α	u	$\lvert\chi\rvert(d = 10000)$	Critical value
0.499	0.249	0.45	1.96
0.502	0.248	0.52	
0.659	0.839	0.57	

Table 6: Results of LC.

α	u	LC	$N/2$
0.499	0.249	498	500
0.502	0.248	501	
0.659	0.839	501	

4 ANALYSIS OF LINEAR COMPLEXITY

It's well-known that an N-bit sequence had better own a linear complexity (abbreviated as LC hereafter) $\lfloor N/2 \rfloor$ or $\lfloor N/2 \rfloor \pm 1$, which is analogous to the behavior of a BSS. With BM algorithm, the LC under the above-mentioned 3 parameter settings (except reducing the length to 1000) are computed, as shown in Table 6.

Table 6 illustrates that the LC of the 3 sequences are all near $N/2$, which is superb.

5 ANALYSIS OF CIPHER SPACE

When the adversary attacks with precision 10^{-8}, then for our 4 system parameters, the cipher space K is:

$$K = (10^8)^4 = 10^{32} \approx 2^{106.3}.$$

Namely, attacking the proposed generator brutally is slightly easier than attacking 128-bit AES. When the precision rises, the difficulty for the adversary increases as well.

6 CONCLUSIONS

Chaotic systems are keenly dependent on parameters and initial values. They're often utilized to construct cryptosystems. This paper presents a novel approach of coupling, i.e. dependent variable harmonically coupling, which is employed to construct a new chaotic system. Afterwards, a PRBG is proposed based on it. Its strong cipher space is slightly larger compared to its independent variable counterpart. Via the five statistic tests, it's clear that our generator could produce pseudorandom binary sequences. The linear complexity of the generated sequences and the cipher space are analyzed as well.

ACKNOWLEDGEMENTS

This work is partially supported by the National Natural Science Foundation of China under Grant No. 61462033, Natural Science Foundation of Jiangxi Province under Grant No.20161BAB202059, the Science and Technology Project of Provincial Education Department of Jiangxi (GJJ160430). Thanks to my supervisors Changxuan Wan and Zuowen Tan.

REFERENCES

1. Bao, Narenmandula, Tubuxin, Eredencang, 2007. Dynamic behavior of complete synchronization of coupled chaotic oscillators. *Acta Phys. Sin.*, 1971-1974.
2. Hu, Liu, Shang, Zhang, 2017. Design and analysis of pseudo-random sequence generator based on spatiotemporal chaos. *Computer Engineering and Applications*, 100-105.

3. Li, Mou, Cai, 2001. Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. In *INDOCRYPT'01, Second International Conference on Cryptology in India*. Springer.
4. Liu, 2008. One-way hash function based on integer coupled tent maps and its performance analysis. *Journal of Computer Research and Development*, 563-569.
5. Liu, Fu, 2007. Spatiotemporal chaotic one-way hash function construction based on coupled tent maps. *Journal on Communications*, 30-38.
6. Liu, Tian, Song, 2006. The synchronization condition of linearly coupled chaotic system. *Acta Phys. Sin.*, 3945-3949.
7. Luo, Qiu, Chen, 2012. Spatiotemporal chaotic pseudorandom number generator based on coupled sawtooth map. *Journal of Shenzhen University Science and Engineering*, 335-340.
8. Ma, Wu, H. Qin, 2013. Realization of synchronization between hyperchaotic systems by using a scheme of intermittent linear coupling. *Acta Phys. Sin.*, 1-8.
9. Qi, Sun, Wang, He, 2017. Design and performance analysis of hyperchaotic pseudo-random sequence generator. *Computer Engineering and Applications*, 135-139.
10. Shannon, 1949. Communication theory of secrecy systems. *Bell System Technical Journal*, 656-715.
11. Tan, Wu, 2008. Study of exponentially cross-coupled chaotic systems for a random bit generator. In *IITA'08, Second International Symposium on Intelligent Information Technology Application*. IEEE Press.
12. Tan, Wu, 2008. Study of linearly cross-coupled chaotic systems for a random bit generator. In *CIS'08, International Conference on Computational Intelligence and Security*. IEEE Press.
13. Wu, 2016. An independent variable exclusively coupled chaotic pseudorandom bit generator. *Computer Engineering & Science*, 2197-2201
14. Wu, 2016. An independent variable exclusively coupled chaotic system for a pseudorandom bit generator. In *ICIICII'16, Second International Conference on Industrial Informatics – Computing Technology, Intelligent Technology, Industrial Information Integration*. IEEE Press.
15. Wu, Tan, Wan, 2011. Harmonically coupled chaotic system for a pseudo-random bit generator. *Journal of Chinese Computer Systems*, 639-643.
16. Wu, Wang, Duan, 2017. A memristor-based time-delay chaotic systems and pseudo-random sequence generator. *Acta Phys. Sin.*, 030502-1-11.
17. Wu, Xia, Pang, Fan, 2007. Simulated study of coupled chaotic systems' spatiotemporal dynamics. *Chinese Journal of Electron Devices*, 1384-1386.
18. Yu, Liu, 2005. Synchronization of symmetrically nonlinear-coupled chaotic systems. *Acta Phys. Sin.*, 3029-3033.