

# Generalized Parabola Chaotic map for Pseudorandom Random Number Generator

Nattagit Jiteurtragool

Department of Computer and Information Sciences, Faculty of Applied Science,  
King Mongkut's University of Technology North Bangkok, Bangkok, 10800, Thailand  
nattagit.j@sci.kmutnb.ac.th

**Abstract**— In this paper, a generalized form of chaotic map based on nonlinear function with parabolic shape is introduced. The study involves the investigation of chaotic dynamics in terms of apparent in time-domain, and both qualitatively and quantitatively examination using bifurcation diagram and Lyapunov exponents. Furthermore, the practical application of these parabolic chaotic maps is showcased in a pseudo-random number generator, with its performance evaluated using statistical tests from the NIST SP800-22 test suite.

**Keywords**— chaotic map, discrete-time chaotic, parabola function, pseudo random number generator, NIST

## I. INTRODUCTION

Chaotic behaviours exist in wide range of both natural and man-made phenomena [1]. Over the years, there has been a remarkable surge of interest in nonlinear systems which exhibit chaotic behaviour, with various areas of applications such as behaviour study, communication, cryptography, and system control [2-4]. The study of chaotic behaviours often involves the use of a discrete-time dynamical model known as a chaotic map.

In the meantime, countless studies of random number generator (RNG), which is a computational or hardware-based mechanism that able to produces a randomness sequence of number, has undergone thorough examination, as random numbers hold a crucial role in cryptography. This scrutiny encompasses intricate mathematical models, numerical simulations, and extensive statistical research. RNG can theoretically divided into 2 categories, true random number generator (TRNG), which mainly relied on physical phenomenal (non-deterministic), and pseudorandom number generator (PRNG), which is mathematical algorithms (deterministic). Classification of RNGs is shown in Fig.1. TRNG mostly relied on non-deterministic phenomena in the nature such as thermal noise, quantum state, electrical noise, even atmospheric noise. These phenomena will then be captured and digitized. Ideally, TRNG is expected to produce results that are unpredictable, and statistically unbiased. In contrast, PRNG, which relied on deterministic system which driven by mathematical algorithms, cannot expect a true randomness result. However, these algorithms, which beginning with an initial seed value in order to produce pseudo-

random sequences, can be characterized by good statistical properties, rapid execution, repeatability, and reproducibility. All things considered, the chaotic map, which is a system that exhibit the property of extremely sensitivity to initial condition, and considered a deterministic system, is a suitable candidate as randomness sources for a pseudorandom random number generator.

Inspired by prior research [5], a generalized form of chaotic map algorithm based on nonlinear function with parabolic shape is presented in this paper. The parabola chaotic map is based on various parabola functions including the absolute value function, which is regarded as a linearized parabolic function, were employed. The chaotic characteristics of the proposed chaotic maps were explored using bifurcation diagram, and Lyapunov exponents. The findings reveal that the parabola chaotic maps demonstrate intermittently chaotic behaviour, while the linearized parabola chaotic map demonstrates robust chaos across a broader spectrum of parameter. Furthermore, to illustrate this concept practically, a pseudo random number generator utilizing parabola chaotic map was also proposed. The resulting random number output is subsequently assessed through the standard NIST SP800-22 test suite.

## II. CHAOTIC MAP

### A. Previous work

In addition to the well-known such as tent map, logistic map and gauss map, the Sigmoidal chaotic map developed in our previous work [5] which described as

$$x_{n+1} = \mp A f_{NL}(B x_n) \pm C x_n \pm D \quad (1)$$

where the parameters A, B, C, and D are real constants,  $x_n$  is a real variable, and  $f_{NL}(x)$  is an S-shaped nonlinear function or so-called sigmoidal. It is seen in (1) that the sigmoidal chaotic map is different from typical chaotic map since this chaotic map can offer different behaviour regarding the utilized sigmoidal function.

### B. Proposed Generalized Parabola Chaotic Map

Motivated by the exiting sigmoidal chaotic map where the nonlinear function can be replaceable by any S-shaped nonlinear functions. This raises the question of “is it possible to

replace the sigmoidal functions with other nonlinear functions in the exiting chaotic map?”. Thoroughly investigations have led to a chaotic map using parabola functions, presented in this paper. The proposed parabola chaotic map can be defined by the simple mathematical model of the form

$$x_{n+1} = \mp A f_{NL}(Bx_n) \pm C \quad (2)$$

where the parameters A, and B are real constants,  $x_n$  is a real variable, and the  $f_{NL}(x)$  is a parabola function. Moreover, it is apparent that the proposed chaotic map in (2) is a conjugation of two chaotic map which can also be expressed as

$$x_{n+1} = A f_{NL}(Bx_n) - C \quad (3)$$

$$x_{n+1} = -A f_{NL}(Bx_n) + C \quad (4)$$

The summarization of the chaotic maps based on (2) using various parabola functions is shown Table I. In term of mathematical, the  $f_1$  and  $f_2$  are polynomial functions with even degree and a Gaussian function, respectively, and  $f_3$  is based on inverse trigonometric function such a hyperbolic cosine. Meanwhile  $f_4$  is an absolute function which considered linearized parabolic shape function.

**TABLE 1.** CHAOTIC MAPS BASED ON PARABOLIC SHAPE NONLINEAR FUNCTIONS  $F_{NL}(X)$

| Parabolic Shape Functions | Descriptions           | Parabola Chaotic Maps                 |
|---------------------------|------------------------|---------------------------------------|
| $f_1(x) = (x)^N$          | Even Degree Polynomial | $x_{n+1} = \mp A(Bx_n)^N \pm C$       |
| $f_2(x) = e^{-x^2}$       | Gaussian Function      | $x_{n+1} = \mp A e^{-(Bx_n)^2} \pm C$ |
| $f_3(x) = \cosh(x)$       | Hyperbolic Cosine      | $x_{n+1} = \mp A \cosh(Bx_n) \pm C$   |
| $f_4(x) =  x $            | Absolute               | $x_{n+1} = \mp A  Bx_n  \pm C$        |

To exploration of chaotic behaviour both qualitatively and quantitatively, a bifurcation diagram and a Lyapunov Exponent (LE) can be used respectively. A bifurcation diagram offers insights into the possible long-term behaviours of a system, including fixed points or periodic orbits, by varying a bifurcation parameter. Conversely, the Lyapunov Exponent, a well-recognized indicator of chaos, serves a metric for assessing chaos by reflecting the average divergence between two closely related trajectories within a dynamic system [6]. The LE equation can be defined as

$$LE = \lim_{n \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \log_2 \frac{dx_{n+1}}{dx_n} \quad (5)$$

where N is the number of iterations. A positive value of LE indicate chaotic behaviours of dynamical systems and the larger value is the higher degree of chaoticity.

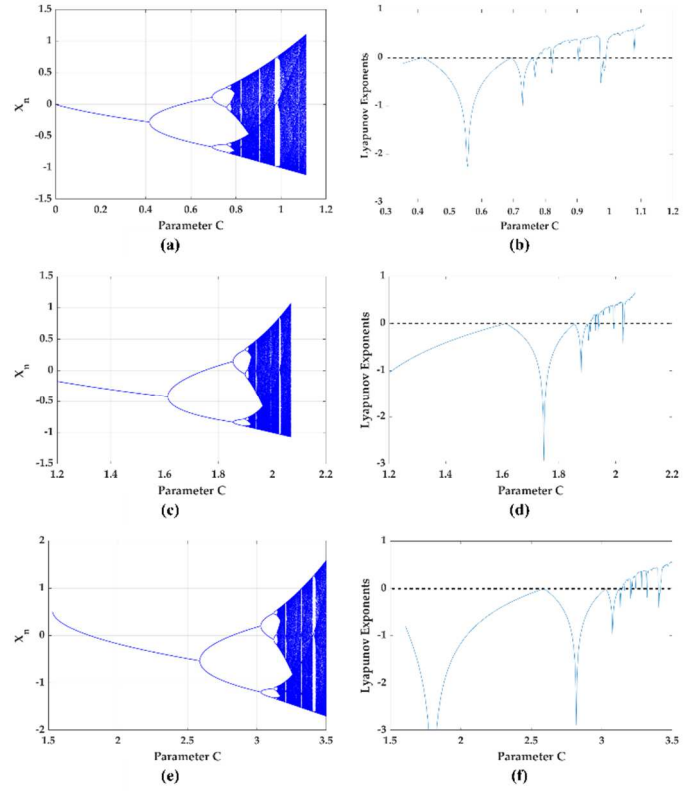


**Figure 1.** Bifurcation diagrams (left) and Lyapunov exponent (LE) plots (right) of the parabola chaotic maps with  $A = 1.8$  and  $B = 1$ ; (a, b) for function  $f_1$ , (c, d) for function  $f_2$ , and (e, f) for function  $f_3$ .

To evaluate the chaotic characteristics and the continuity of the proposed parabolic chaotic maps defined in Equation (3), both bifurcation diagrams and LE plots were utilized, as depicted in Fig. 1. For this investigation, parameters A and B were set to 1, while parameter C was used as a bifurcation parameter. The bifurcation diagrams in Figs. 1a, 1c, and 1e illustrate a shared chaotic behaviour among the parabolic chaotic maps corresponding to functions  $f_1$  through  $f_3$ . It is noticeable that these bifurcation diagrams reveal periodic windows and demonstrate discontinuous chaotic behaviour, aligned with the observations in the LE plots. However, this implies that, across all three cases offer robust chaos for some portion of parameter C.

In addition to the utilization of nonlinear functions with parabolic transfer characteristics, the proposed parabolic chaotic map can also integrate a triangular function, such as an absolute value function, which can be seen as a linearized variant of the parabolic function. Figure 2 provides a visual representation of the bifurcation diagram and LE plot for the parabolic chaotic map based on the absolute value in Equation (8). In this depiction, parameter A were carefully chosen to serve as the variable responsible for generating the bifurcation, while parameters B and C remain set at 1. As observed in the corresponding LE plot, the bifurcation diagram of the linearized parabolic chaotic map consistently exhibits chaotic behaviour across the entire range of parameter A.

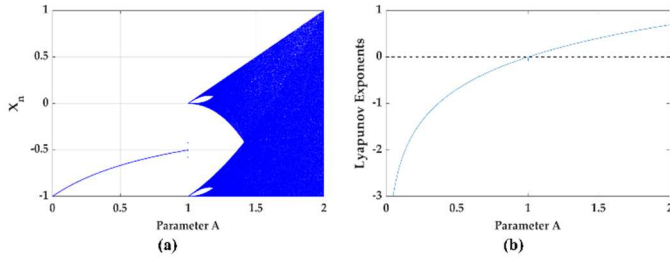


**Figure 2.** Bifurcation diagrams (left) and Lyapunov exponent (LE) plots (right) of absolute value function based parabola chaotic map at specified parameters  $B = 1$  and  $C = 1$ .

### III. DESIGN AND ANALYSIS OF PSEUDORANDOM RANDOM NUMBER GENERATOR

#### A. Random Number Generator

As mentioned, a RNG is a computational algorithm or device that generates numbers or sequences of numbers that appears random or unpredictable. While there are two primary types of RNGs one is True Random Number Generators (TRNGs) and the other is Pseudo-Random Number Generators (PRNGs). These random number generators still share common structure which consisted of several key components that work together as shown in Fig.3.

| Entropy Source                                                                                                                                                                                 | Entropy Harvester                                                                                                                                                 | Post Processor                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- Electrical Noise</li> <li>- Quantum Signal</li> <li>- Thermal Noise</li> <li>- Atmospheric Noise</li> <li>- Chaotic Signal</li> <li>- ....</li> </ul> | <ul style="list-style-type: none"> <li>- Periodic Sampling</li> <li>- Nonuniform Sampling</li> <li>- Comparator</li> <li>- D-Flip Flop</li> <li>- ....</li> </ul> | <ul style="list-style-type: none"> <li>- Von Neumann</li> <li>- XOR</li> <li>- LFSR</li> <li>- Bit Skipping</li> <li>- Quasi-Shift Register</li> <li>- ....</li> </ul> |

**Figure 3.** Typical structure of a random number generator.

The key element in any RNG is the entropy source, which is crucial for providing unpredictability and serves as the foundation of RNG security. The role of the entropy harvester was significant in efficiently gathering the raw signal without compromising the integrity of the entropy source. It reads the data generated by the entropy source and converts it into a series of bits, which are referred to as raw bit data. Although, the output from the entropy harvester comprises a random bit sequence, these raw bits sequence often exhibit bias and lack of uniform distribution. Therefore, a post-processor remains necessary to rectify this issue, ensuring that the output becomes uniformly distributed and addressing any statistical imperfections in the generated sequences. Even though the result from the entropy harvester is a random bit sequence, the raw bits are usually biased and not uniformly distributed for various reasons. Therefore, the post-processor is still required to make output uniformly distributed as well as improve the statistical imperfections of the generated sequences.

#### B. Pseudorandom Random Number Generator based on Generalized Parabola Chaotic Map

The classification of a chaotic-based random number generator as a TRNG or a PRNG is depended on its specific implementation. When a chaotic based random number

generator employs unpredictable physical processes like the chaotic behaviour of electronic circuits or the unpredictability of systems such as a double pendulum to produce random numbers, it qualifies as a TRNG. This is due to its reliance on inherently unpredictable physical phenomena to generate genuine randomness. On the contrary, if the chaotic-based random number generator employs a deterministic algorithm to mimic chaotic behaviour such as chaotic map equation to establish an initial seed value, subsequently using algorithms to generate a sequence of numbers, it falls into the category of PRNG.

In order to construct PRNG based on generalized parabola chaotic map, architecture is shown in Fig.4. The proposed architecture of the PRNG consisted of the absolute value function based parabola chaotic map as an entropy source, a comparator with threshold value used as an entropy harvester to turn raw output signal from chaotic map into raw bit data.

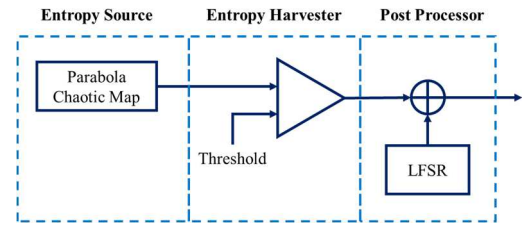


**Figure 4.** The proposed architecture of Pseudorandom Random Number Generator based on Generalized Parabola Chaotic map.

The selection of the comparator's threshold value is a deliberate process. Shannon's entropy is employed to assess the impact of this threshold and the resulting level of entropy, essentially measuring the system's randomness. Shannon's entropy can also be defined as follows:

$$H = -\sum_{i=0}^1 P_i \log_2 P_i \quad (6)$$

The calculated entropy over the range of parameter threshold is depicted in Figure 5(a).

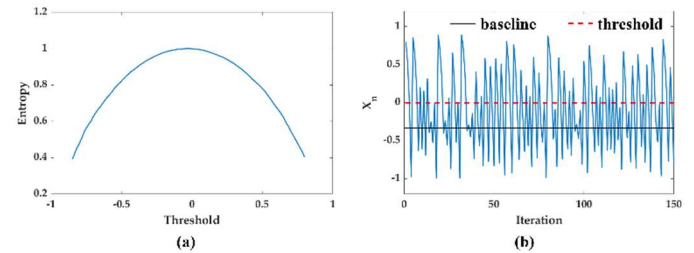


**Figure 5.** Typical structure of a random number generator.

Through, Chaos signals are characterized by their sensitivity to initial conditions, non-periodic behavior, and a broad range of frequency components, the plot of chaotic waveforms in time-domain, as shown in Figure 5(b), suggest that the baseline value fall between 0 and 0.5. Nevertheless, it's noticeably from the plot of entropy versus threshold indicate the value of threshold differences from the baseline.

As for the post processor, an 8-bit Fibonacci linear feedback shift register (LFSR) were selected. Fibonacci linear feedback

shift register is a chain of shift registers where the inputs are linear function of their previous state. It's referred to as a "Fibonacci" LFSR as it employs a linear combination of its internal bits, similar to the mathematical Fibonacci sequence. In order to enhance the statistical properties of PRNG, the generated raw bit data then combined with the LFSR post processor through using exclusive-or (XOR) operation.

### C. Randomness Evaluation

Although there are many evaluations for random number generator, the random bit output of the proposed PRNG has been examined, in terms of statistical properties, using the standard NIST SP800-22 test suite. The NIST test suite, which issued by the National Institute of Standards and Technology, is a statistical test consists of 15 tests [7]. The NIST test suite also generally accepted as a standard test suit for both TRNG and PRNG. The test can be used to analyse the number sequence by identifying any pattern of value that indicates non-randomness within the sequences. This is achieved through the assessment of probability values (P-value), a valuable metric for determining statistical property of each test. The P-value indicates a randomness of the test sequences where the P-value exceeds 0.01, the sequence can be confidently regarded as random and accepted. Conversely, if the p-value is below this threshold, the sequence is considered as non-random.

**TABLE 2.** NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) STATISTICAL TEST SUITE.

| Test Methods               | P-value | Pass Ratio | Result |
|----------------------------|---------|------------|--------|
| Frequency                  | 0.6255  | 1.00       | Pass   |
| Block Frequency (m=128)    | 0.9307  | 1.00       | Pass   |
| Runs                       | 0.5236  | 1.00       | Pass   |
| Longest Run                | 0.2717  | 1.00       | Pass   |
| Binary Matrix Rank         | 0.3534  | 1.00       | Pass   |
| Discrete Fourier Transform | 0.9487  | 1.00       | Pass   |
| Non-overlapping Template   | 0.0734  | 1.00       | Pass   |
| Overlapping Template       | 0.9131  | 1.00       | Pass   |
| Universal Statistical      | 0.1121  | 1.00       | Pass   |
| Linear Complexity          | 0.3230  | 1.00       | Pass   |
| Serial (1)                 | 0.5057  | 1.00       | Pass   |
| Serial (2)                 | 0.6735  | 1.00       | Pass   |
| Approximate Entropy        | 0.3009  | 1.00       | Pass   |
| Cumulative Sums            | 0.7857  | 1.00       | Pass   |
| Random Excursions          | 0.7535  | 1.00       | Pass   |
| Random Excursions Variant  | 0.6339  | 1.00       | Pass   |

The statistical properties of the proposed PRNG were evaluated using 10 Mbit data. The generated bit sequence is divided into 10 sequences with the length of 1Mbit for each block. The calculated P-values for ever test of the NIST is shown in Table 2. The tests result has shown that the proposed PRNG can pass all the statistical tests of the NIST.

## IV. CONCLUSION

Chaotic map played an important role in various field of application such as information security and cryptography. In this paper, A generalized chaotic map based on parabola functions. Chaotic dynamics were described in terms of apparent in time-domain, and both qualitatively and

quantitatively examination using bifurcation diagram and Lyapunov exponents. The PRNG which utilized the proposed parabola chaotic maps were also demonstrated and evaluation result of the random bit sequences were evaluated using the standard NIST SP800-22 test suite and pass all the tests.

## REFERENCES

- [1] Jensen, Roderick V, "Classical Chaos." *American Scientist*, vol. 75, no. 2, 1987.
- [2] M. Rosalie, et al, "Chaos-enhanced mobility models for multilevel swarms of UAVs," *Swarm and Evolutionary Computation*, 41, 2018, p.36-48.
- [3] Kaddoum, Georges, "Wireless chaos-based communication systems: A comprehensive survey," *IEEE Access*, 4, 2016, pp.2621-2648.
- [4] Fradkov, Alexander L., and Robin J. Evans., "Control of chaos: Methods and applications in engineering," *Annual reviews in control*, 29(1), 2005, p. 33-56.
- [5] Jiteurtragool N, Masayoshi T., and San-Um W., "Robustification of a one-dimensional generic sigmoidal chaotic map with application of true random bit generation," *Entropy*, 20(2),2018, p. 136.
- [6] Abarbanel, Henry DI, Reggie Brown, and M. B. Kennel, "Lyapunov exponents in chaotic systems: their importance and their evaluation using observed data," *International Journal of Modern Physics B*, 5(09), 1991, p. 1347-1375.
- [7] A. Rukhin, et al, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *National Institute of Standards and Technology (NIST)*, special publication 800-22, August 2008.
- [9] Cicek, Ihsan, Ali Emre Pusane, and Gunhan Dundar, "A novel design method for discrete time chaos based true random number generators," *Integration*, 47(1), 2014, p. 38-47.
- [10] Stipčević, Mario, and Çetin Kaya Koç, "True random number generators," *Open Problems in Mathematics and Computational Science*, Cham: Springer International Publishing, 2014.
- [11] Yu, Fei, et al, "A survey on true random number generators based on chaos," *Discrete Dynamics in Nature and Society*, 2019.