15

An Improved PRNG Based on the Hybrid between One- and Two- Dimensional Cellular Automata

Sang-Ho Shin[1] and Kee-Young Yoo[2]
[1]*School of Electronic Engineering and Computer Science, Kyungpook National University*
Gyengdaejeongmunro 67, Buk-Gu, Daegu, 702-701
[2]*School of Computer Science and Engineering, Kyungpook National University*
Gyengdaejeongmunro 67, Buk-Gu, Daegu, 702-701
South Korea

1. Introduction

Cellular automata (CA) were initiated in the early 1950s to develop complex structures of capable self-reproduction and self-repair. Since then many researchers have taken attend in the study of CA. Initially, CA concept was first introduced by von Neumann von Neumann (1966) for the proposal of modeling biological self-reproduction. His primary interest was to derive a computationally universal cellular space with self-reproduction configurations. Afterward, a new phase of activities was started by Wolfram Wolfram (1983; 1984), who pioneered the investigation of CA as a mathematical model for self-organizing statistical systems. Wolfram was proved that the randomness of the patterns generated by maximum-length CA is significantly better than other widely used methods, such as linear feedback shift registers. The intensive interest in this field can be attributed to the phenomenal growth of the VLSI technology that permits cost-effective realization of the simple structure of local-neighborhood CA Wolfram (1986).

The PRNGs based on CA have been studied for the last decade and a variety of CA PRNGs have been proposed Guan & Tan (Jul. 2004); Guan & Zhang (Feb. 2003); Seredynski et al. (2004); Tan & Guan (2007); Xuelong et al. (Oct. 2005). Recent interest has been focused on the two-dimensional (2-D) CA PRNGs with genetic algorithm Chowdhury et al. (1993); Guan et al. (2004); Quieta & Guan (2005); Tomassini et al. (2000), since, statistically, the point has been established that the quality of randomness of a 2-D CA is significantly better than a 1-D CA.

In this paper, an efficient PRNG based on hybrid between one-dimension (1-D) and two-dimension (2-D) CA is proposed. In the phase of the evolution of 2-D CA cells, the proposed CA PRNG is based on von Neumann neighborhood, in that this method refers to the five cells and new control values (rule decision input value & linear control input value) to decide a rule. In the phase of the evolution of 1-D CA cells, on the other hand, $<90, 150>$ rule combination is used because this rule combination is better than the others Hortensius et al. (1989). In the meantime, the proposed CA PRNG is compared with previous works Guan et al. (2004); Tomassini et al. (2000) to check the quality of randomness. The proposed CA PRNG could generate a good quality of randomness because the proposed CA PRNG is better than

Neighborhood state	111	110	101	100	011	010	001	000	rule number
Next state	0	1	0	1	1	0	1	0	90
Next state	0	0	0	1	1	1	1	0	30
Next state	1	0	0	1	0	1	1	0	150
Next state	1	1	0	0	1	0	1	0	202

Table 1. The examples of the state transition for rules with 2-state, 3-neighborhood

Rule number	Combination Logic gate
$30(=2^4+2^3+2^2+2^1)$	$s_{i-1}(t) \oplus (s_i(t) \vee s_{i-1}(t))$
$90(=2^6+2^4+2^3+2^1)$	$s_{i-1}(t) \oplus s_{i+1}(t)$
$150(=2^7+2^4+2^2+2^1)$	$s_{i-1}(t) \oplus s_i(t) \oplus s_{i+1}(t)$
$202(=2^7+2^6+2^3+2^1)$	$s_{i-1}(t) \wedge (s_i(t) \oplus s_{i+1}(t))$

where $\oplus$, $\vee$ and $\wedge$ are the Boolean operations XOR, OR and AND, respectively.

Table 2. The combination logic gates correspond with rule numbers

the previous works and passed by the ENT Walker (Oct., 1998) and DIEHARD Marsaglia (1998) test suite.
The rest of this paper is organized as follows. In Section 2, related work is briefly reviewed. The hybrid CA PRNG is proposed in Section 3. Section 4 analyze the proposed CA PRNG. Section 5 shows the experimental results. Section 6 provides a conclusion.

2. The related works

In this section, the concepts of cellular automata will be introduced.

2.1 One-dimension CA

A CA is a dynamical system in which space and time are discrete. A CA consists of an array of cells, each of which can be in one of a finite number of possible states, updated synchronously in discrete time steps, according to a local identical interaction, a rule. The next state of a cell is assumed to depend on itself and on its neighbors. The cells evolve in discrete time steps according to some deterministic rule that depends only on local neighbors.
The next-state function for a three-neighborhood CA cell in one-dimension can be expressed as following equation (1):

$$s_i(t+1) \;=\; f(\, s_{i-1}(t),\; s_i(t),\; s_{i+1}(t)\,) \tag{1}$$

where f denotes the local function realized with a combinational logic, such as AND, OR, XOR, and NOT, i is the position of an individual in the one-dimensional array of the cell, t is the tth time step, $s_i(t)$ is the output state of the ith cell at the tth time step, and $s_i(t+1)$ is the output state of the ith cell at the $(t+1)$th time step.
In a two-state, three-neighborhood CA there can be a total of 2^3 (from 000 to 111) distinct neighborhood configurations. For such a CA there can be a total of $2^{2^3}(=256)$ distinct mappings from all these neighborhood configurations to the next state. Each mapping is called a rule of CA. If the next-state function of a cell is expressed, then the decimal equivalent of the output is conventionally called the rule number for the cell Wolfram (1986).

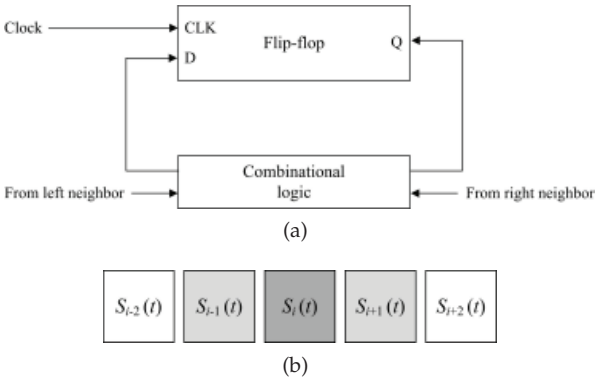

Fig. 1. A CA cell structures: (a) a 2-state, 3-neighborhood CA cell, (b) an example of CA cells with 3-neighborhood in 1-D

Table 1 expresses the state transition for arbitrary rules with 2-state, 3-neighborhood. In Table 1, the top row gives all eight possible states of the three neighboring cells (the left, right neighbor of the ith cell, the ith cell itself) at the time t. The second to fifth rows give the corresponding states of the ith cell at time $t+1$ for four CA rules. Table 2 shows that the combination logic gates correspond with rule numbers. In Table 2, rule numbers consist of sum which is converted decimal number of neighborhood states from 111(=MSB) to 000(=LSB). For rule 30, the next state of $111(=2^7)$, $110(=2^6)$, $101(=2^5)$, $100(=2^4)$, $011(=2^3)$, $010(=2^2)$, $001(=2^1)$ and $000(=2^0)$ are 0, 0, 0, 1, 1, 1, 1 and 0, respectively. Hence, $2^7 \times 0 + 2^6 \times 0 + 2^5 \times 0 + 2^4 \times 1 + 2^3 \times 1 + 2^2 \times 1 + 2^1 \times 1 + 2^0 \times 0 = 30$.
A CA is said to be a *Null Boundary CA* (NBCA) if the left (or right) neighbor of the leftmost (or rightmost) terminal cell is connected to the logic 0-state, or a *Periodic Boundary CA* (PBCA) if the extreme cells are adjacent to each other. Figure 2 shows the features of each boundary CA.

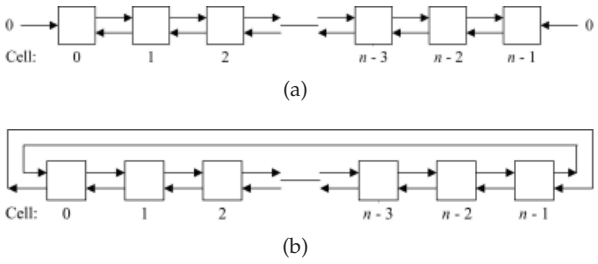

Fig. 2. The features of each boundary CA: (a) Null boundary CA, (b) Periodic boundary CA

2.2 Two-dimension CA

A two-dimension (2-D) CA is a generalization of a 1-D CA, where the cells are arranged in a two-dimensional grid with connections among the neighboring cells. For a 2-D CA, types of cellular neighborhoods are usually considered: five cells, consisting of one cell along with its four immediate non-diagonal neighbors (also known as the von Neumann neighborhood); and nine cells, consisting of one cell along with its eight surrounding neighbors (also known

as the Moore neighborhood). In this paper, a type of von Neumann neighborhood is used which considers five-neighborhoods that these consist of *self*, *top*, *bottom*, *left* and *right*.

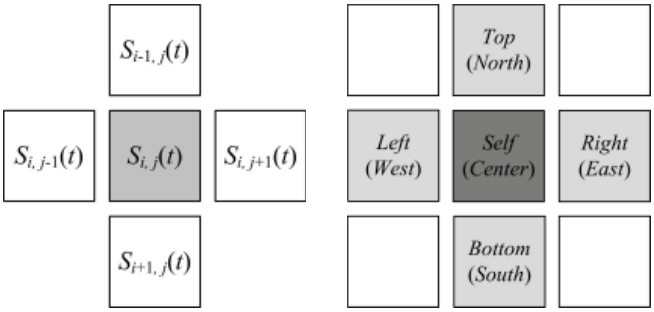

Fig. 3. The geometric representation of the von Neumann neighborhood.

Figure 3 shows the type of von Neumann neighborhood with a five-neighborhood dependency.
The next state $s_{i,j}(t+1)$ of a 2-D CA is given by

$$s_{i,j}(t+1) = f(s_{i-1,j}(t), s_{i,j-1}(t), s_{i,j}(t), s_{i,j+1}(t), s_{i+1,j}(t)). \quad (2)$$

Since f is a Boolean function of five variables, there are 2^5 = 32 distinct neighborhood configurations. Hence to express a transition rule of a 2-D CA in a manner similar to a 1-D CA, 32-bits are considered which is almost impossible to manage practically.

2.3 The previous works

In this section, previous CA PRNGs are described. Tomassini et al. have been proposed 2-D CA PRNG based on an 8×8 structure Tomassini et al. (2000) and Guan et al. have proposed 2-D CA PRNGs based on asymmetric neighborhood Guan et al. (2004). In the final phase, these PRNGs are constructed by using the evolutional method which is called a genetic algorithm Steeb (2001). A genetic algorithm is an iterative procedure that involves a constant-size population of individuals, each one represented by a finite string of symbols (known as the genome), encoding a possible solution in a given problem space. A genetic algorithm has operators that are a crossover, and mutation and a has fitness function. Iterating this procedure, the genetic algorithm may eventually find an acceptable solution. Hence, a genetic algorithm provides a high randomness quality, but has problems that include high time complexity for the evolution of CA cells.
In Tomassini et al.'s PRNG Tomassini et al. (2000), every cell of the evolving CA assigns a fitness function value and rule number which decides the result of the evolved cell by the fitness function value. Also, to raise the quality of randomness, they used a genetic algorithm. Guan et al.'s PRNGs Guan et al. (2004) are constructed from a asymmetric neighborhood (5×10) CA structure for reducing the number of cells. Similarly, they used a genetic algorithm. To evaluate the randomness quality of the proposed CA PRNG, in this paper, the sequence of the proposed PRNG (PRNS) will be compared with above two CA PRNS.

Cells		XOR logic
0	0	0
0	1	1
1	0	1
1	1	0

Table 3. The result of operation of XOR logic for two cells

3. The proposed hybrid CA PRNG

In this section, the proposed scheme is explained.

3.1 The method of deciding the rules for 1-D & 2-D

First of all, the rule of CA cell for 2-D are considered. A hybrid CA PRNG based on the von Neumann neighborhood method is proposed. The number of rules in this method is 2^{32} because there are 32 distinct neighborhood configurations. In this paper, the XOR logic is considered because the frequencies of occurrence of 0 for the operation of XOR is 2, in four cases given in the Table 2. From this fact, it can be guessed that the binomial distribution for the probability of XOR is $X \sim B(n, \frac{1}{2})$, where n is independent Bernoulli trials. That is, the expected value of the binomial distribution of the frequencies of occurrence of 0 for a XOR is decided by n.

Let $s_{i,j}(t)$ be a state value of the cell at row i, column j, and time t. Its state value at the next step, $s_{i,j}(t+1)$ is then computed as the following equation (3):

$$\begin{aligned} s_{i,j}(t+1) = X \ \oplus \ & (C \wedge s_{i,j}(t)) \\ & \oplus (N \wedge s_{i-1,j}(t)) \ \oplus \ (W \wedge s_{i,j-1}(t)) \ \oplus \ (E \wedge s_{i,j+1}(t)) \ \oplus \ (S \wedge s_{i+1,j}(t)) \end{aligned} \tag{3}$$

where $\oplus$ and $\wedge$ are the Boolean operations XOR and AND, respectively. X, C (center), N (north), S (south), W (west), and E (east) are binary variables (that is, 0 or 1). C, N, S, W, and E denote whether the respective neighboring cell state is taken into account (a value of 1) or not (a value of 0). The binary variable X distinguishes between linear (X = 0) and nonlinear (X = 1) rules. For example, rule 14 (001110), that is, $(X||C||N||W||E||S)$ is represented as follows :

$$s_{i,j}(t+1) = s_{i-1,j}(t) \oplus s_{i,j-1}(t) \oplus s_{i+1,j}(t).$$

Next, the rule of CA cell for 1-D with 2-state, 3-neighborhood is considered. A rule is chosen which is $<90, 150>$ in this paper. The logic of this rules consists of XOR which has $X \sim B(n, \frac{1}{2})$. Moreover, the rule combination of $<90, 150>$ has been proved to have a high randomness quality by Hortensius et al.'s paper Hortensius et al. (1989). Figure 4 shows the structure of rule $<90, 150>$ for a cell in 1-D CA.

The Boundary is considered. Generally, a PBCA is frequently applied, resulting in a circular grid for 1-D case and in a doughnut for the 2-D case. A NBCA can also be used, in which the grid is surrounded by an outer layer of cells of zero. In this paper, a PBCA is chosen to raise the quality of randomness.

3.2 Hybrid between 1-D and 2-D CA PRNG

Figure 4, 5 and 6 show the process & structure of the proposed CA PRNG, respectively. One round consists of four phases. The process step-by-step is summarized as follows.

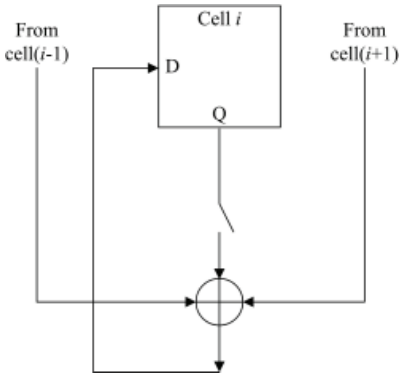

Fig. 4. The structure of rule <90, 150>

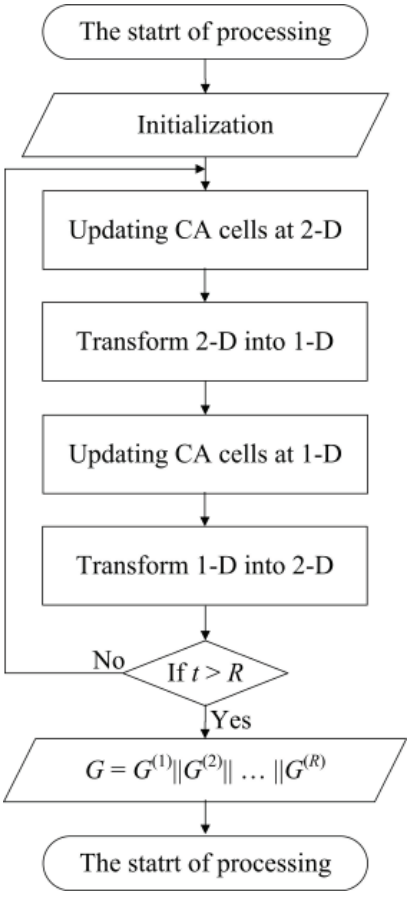

Fig. 5. The process of the proposed CA PRNG

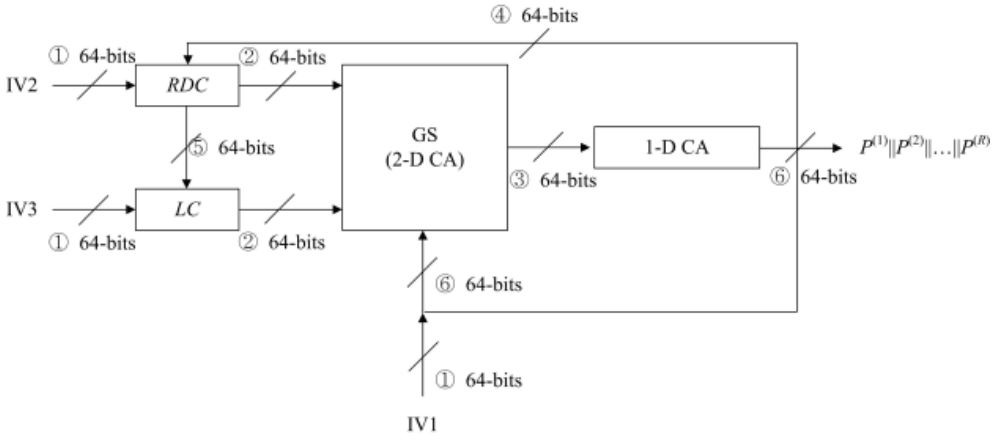

Fig. 6. The structure of the proposed CA PRNG

3.2.1 Initialization

The 192-bit initial seed is randomly generated. The seed, then, divides into three parts, from 0^{th} to 63^{th} (=IV_1), from 64^{th} to 127^{th} (=IV_2) and from 128^{th} to $final$ bit (=IV_3). The initial values IV_1, IV_2, and IV_3 are stored in $GS^{(0)}$ (GS: Global state, consists of the 8×8 2-D CA cells and the first row is from 0^{th} to 7^{th}, the second row is from 8^{th} to 14^{th}, ... , the final row is from 57^{th} to 63^{th}), $RDC^{(0)}$ (rule decision control unit, consists of 64-bit 1-D CA cells) and $LC^{(0)}$ (linear control unit, consists of 8×8 2-D CA cells and the first row is from 0^{th} to 7^{th}, the second row is from 8^{th} to 14^{th}, ... , the final row is from 57^{th} to 63^{th}), respectively.

3.2.2 Updating at 2-D

The rule $r_{i,j}(t)$ is decided by $RDC^{(t)}$ which is decided by self, left 2 bits, and right 2 bits (that is, $s_{i-2}(t)$, $s_{i-1}(t)$, $s_i(t)$, $s_{i+1}(t)$, and $s_{i+2}(t)$ at t-th time step). Then, generate the next state $GS^{(t+1)}$ by $r_{i,j}$, $LC^{(t)}$, and $GS^{(t)}$ and represents the equation (4):

$$GS^{(t+1)} = f(r_{i,j}, LC^{(t)}, GS^{(t)}), \tag{4}$$

where R is a repeating counter for producing PRNS of a demanded cycle length, $0 \leq t \leq R$, $0 \leq i, j \leq 7$.

3.2.3 Transform 2-D into 1-D

The generated state $GS^{(t+1)}$ transforms 2-D into 1-D because of applies to the 1-D CA rule <150,90>. The method is that each row in $GS^{(t+1)}$ concatenates 64-bits stream as in the following equation (concatenation is denoted "||") (5):

$$TGS^{(t+1)} = \bigcup_{i=0,\, j=0}^{7} s_{i,j}(t+1) = s_{0,0}(t+1)||s_{0,1}(t+1)||...||s_{7,7}(t+1), \tag{5}$$

where $s_{i,j}(t+1)$ indicates each cell in $GS^{(t+1)}$ and $TGS^{(t+1)}$ (TGS: Transformed GS) indicates transform 2-D into 1-D in $GS^{(t+1)}$.

$s_{i-1}(t)$	$s_i(t)$	$s_{i+1}(t)$	rule 90	rule 150
0	0	0	0	0
0	0	1	1	1
0	1	0	0	1
0	1	1	1	0
1	0	0	1	1
1	0	1	0	0
1	1	0	1	0
1	1	1	0	1

Table 4. The results of the operation of rule 90 & rule 150 for three cells in 1-D

3.2.4 Updating at 1-D

In order to raise the quality of randomness, the combination <90, 150> is used. This rule provides a high randomness quality Hortensius et al. (1989). This method uses the following equation (6):

$$ATGS^{(t+1)} = f_{<90,150>}(s_{i-1}(t+1), s_i(t+1), s_{i+1}(t+1)), \tag{6}$$

where $s_i(t+1)$ is cell at $TGS^{(t+1)}$ in 1-D, $ATGS^{(t+1)}$ is applied to the $TGS^{(t+1)}$ by function f based on rule 90 and 150.

3.2.5 Transform 1-D into 2-D

The updated state transforms 1-D into 2-D because of the application of the 2-D rule. The 64-bit streams are divided into each row by modulo 8 as the following equation (7):

$$GS^{(t+1)} = \bigcup_{i=0,j=0}^{7} s_{i,j}(t+1), \tag{7}$$

where $s_{i,j}(t+1) = s_i(t+1)$, i is that values of 0∼7, 8∼15,..., 57∼63 replace 0, 1,..., 7, respectively. And $j = i \pmod 8$, $(0 \leq i \leq 63)$ in 1-D CA state. Then, RDC and LC replace the new values. The method is represented as the following equation.

$$\begin{aligned} LC^{(t+1)} &= RDC^{(t)} \oplus LC^{(t)}, \\ RDC^{(t+1)} &= GS^{(t)} \oplus GS^{(t+1)}_{(updated\ at\ 1-D\ CA)}. \end{aligned} \tag{8}$$

Lastly, t is increased by 1. If t is greater than R, the phase is finished. Otherwise, go back to the beginning of the 2-D phase.

4. Analysis

In this section, the high quality of randomness of the hybrid CA PRNG is proved. The proposed CA PRNG was evolved by rule <90, 150> in 1-D. Abovementioned rule 90 & 150 consist of combinations of XOR logic, that is, $s_{i-1}(t) \oplus s_{i+1}(t)$ & $s_{i-1}(t) \oplus s_i(t) \oplus s_{i+1}(t)$, respectively. The frequencies of occurrence of 0 or 1 for operation of rule 90 or rule 150 is 4, in eight cases in Table 4. Table 4 shows the results of the operation of a rule 90 & a rule 150 for three cells which are $s_{i-1}(t)$, $s_i(t)$ and $s_{i+1}(t)$. Hence, $E(X)$ (expectation value) of the binomial distribution for a rule 90 or a rule 150 is $\frac{n}{2}$, where n is the number of evolutions in

X	$s_{i-1,j}(t)$	$s_{i,j-1}(t)$	$s_{i,j}(t)$	$s_{i,j+1}(t)$	$s_{i+1,j}(t)$	XOR logic
0	0	0	0	0	0	0
0	0	0	0	0	1	1
0	0	0	0	1	0	1
0	0	0	0	1	1	0
	⋮		⋮		⋮	⋮
1	1	1	1	1	0	1
1	1	1	1	1	1	0

Table 5. The results of the rule operation of all case for six cells in 2-D

Test No.	Test Name	The average value		
		Tomassini et al.	Guan et al.	Proposed
1	Entropy (Close to 8.0)	7.99971	7.99983	7.99991
2	Chi-square (Close to 1.0)	0.989412	0.992002	0.999283
3	SCC (Close to 0.0)	0.000227	0.000171	0.000062

Table 6. The average values of ENT test

1-D. Therefore, the meaning of this proposition shows that rule 90 & rule 150 provide a high quality randomness in terms of 1-D CA PRNG.

Next, the rules of CA cell for 2-D are considered. The proposed CA PRNG used von Neumann neighborhood method and evolved by $RDC^{(t)}$ and $LC^{(t)}$ for next state. $RDC^{(t)}$ consists of five cells ($s_{i-1,j}(t)$, $s_{i,j-1}(t)$, $s_{i,j}(t)$, $s_{i,j+1}(t)$ and $s_{i+1,j}(t)$) and combinations of XOR logic. Hence, the rule of 2-D CA cell consists of 1 bit for linear control bit, 5 bits for rule decision control and combinations of XOR logic, and expresses as equation (3). Table 5 shows the results of the rule operation of all case for six cells in 2-D. Meanwhile, a rule 0 and a rule 128 are not consider in the proposed CA PRNG because the occurrence rate of these rules are very few. Hence, $E(X)$ (expectation value) of the binomial distribution for the rule of 2-D CA cell is $\frac{n}{2}$, where n is the number of evolutions in 2-D. Similarly, the meaning of this proposition shows that provide a high quality randomness in terms of 1-D CA PRNG.

5. Experimental results

In this section, the efficiency of the hybrid CA PRNG is analyzed. To analyze, ENT Walker (Oct., 1998) and DIEHARD Marsaglia (1998) test suites are used. ENT test is useful for evaluating pseudorandom number generators for encryption and statistical sampling applications, compression algorithms, and other applications where the information density of a file is of interest Walker (Oct., 1998). ENT test is a collective term for three tests which are the Entropy test, Chi-square test, and Serial correlation coefficient (SCC) test.

The DIEHARD test suite is important because it seems to be the most powerful and difficult test suite to pass. This test consists of 18 different and independent statistical tests. The result of each test is called p-value. Most of the tests return a p-value in DIEHARD, which should be uniform if the input file contains truly independent random bits. For any given test, a smaller p-value means a better result.

The proposed CA PRNG produces a 64-bit output sequence at each round. The DIEHARD test suite requires a minimum of 10 MB of random number sequences Marsaglia (1998).

Test No.	Test Name	The results of tests (Pass or Fail)			
		Shift register	Tomassini et al.	Guan et al.	Proposed
1	Birthday Spacing	Pass	Pass	Pass	Pass
2	Over. 5-Per.	Pass	Fail	Fail	Pass
3	Binary Rank 31×31	Pass	Pass	Pass	Pass
4	Binary Rank 32×32	Fail	Pass	Pass	Pass
5	Binary Rank 6×8	Pass	Pass	Pass	Pass
6	Bitstream	Pass	Pass	Pass	Pass
7	OPSO	Pass	Pass	Pass	Pass
8	OQSO	Pass	Fail	Fail	Pass
9	DNA	Pass	Pass	Pass	Pass
10	Count-The-1's 01	Fail	Fail	Pass	Pass
11	Count-The-1's 02	Fail	Pass	Fail	Pass
12	Parking Lot	Pass	Pass	Pass	Pass
13	Minimum Distance	Pass	Pass	Pass	Pass
14	3DS Spheres	Pass	Pass	Pass	Pass
15	Squeeze	Pass	Pass	Pass	Pass
16	Overlapping Sums	Pass	Pass	Pass	Pass
17	Runs	Fail	Fail	Pass	Pass
18	Craps	Pass	Pass	Pass	Pass

Table 7. The results of DIEHARD test in p-value pass rate $\geq$ 90% for PBCA

Therefore, the proposed PRNG needs $(10^7 \times 8) \div 64$ time steps for the DIEHARD test. On the other hand, the ENT test suite requires fewer numbers, but the test is executed with the same 10 MB sequence for convenience and the next DIEHARD test. A total of 100 experiments are performed for the ENT and DIEHARD test suite. Table 6 and 7 show the average values of ENT test and the results of DIEHARD test. A pass is considered when all the p-values are passed by more than 90% at the 0.05 level. As the results show in Tables, it is obvious that the quality of randomness of the proposed scheme is better than other different scheme. Additionally, we have performed the boundary CA tests for 1-D & 2-D, and the results of these tests show Table 8 & 9. In Table 8, PB and NB indicate PBCA and NBCA, respectively. The randomness quality of the rule 90 & 150 $(=<90, 150>)$ are better than rule 30, 45. Also, The randomness quality of the PBCA is better than the NBCA. Similarly, The randomness quality of the PBCA is better than the NBCA in 2-D.

6. Conclusion

In this paper, an efficient PRNG was proposed based on the hybrid between 1-D and 2-D CA. To better randomness quality, the *RDC* and the *LC* units were used. As a result, the various types of von Neumann neighborhood and $<90, 150>$ rule combination provide few correlation coefficients for each cell in state $GS^{(t)}$ and a high randomness quality by ENT and DIEHARD test suites (average pass rate more than 90% at the 0.05 level).

7. Acknowledgments

We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. This research was supported by 2nd Brain Korea 21 Project in 2010 and Basic

Test No.	Test Name	The results of tests (Pass or Fail)			
		rule 30(PB)	rule 45(PB)	<90, 150>(PB)	<90, 150>(NB)
1	Birthday Spacing	Pass	Pass	Pass	Pass
2	Over. 5-Per.	Pass	Pass	Pass	Pass
3	Binary Rank 31×31	Pass	Pass	Pass	Pass
4	Binary Rank 32×32	Pass	Pass	Pass	Pass
5	Binary Rank 6×8	Pass	Pass	Pass	Pass
6	Bitstream	Pass	Pass	Pass	Pass
7	OPSO	Fail	Fail	Pass	Pass
8	OQSO	Fail	Fail	Pass	Fail
9	DNA	Pass	Fail	Pass	Fail
10	Count-The-1's 01	Fail	Fail	Pass	Pass
11	Count-The-1's 02	Fail	Fail	Pass	Pass
12	Parking Lot	Pass	Pass	Pass	Pass
13	Minimum Distance	Pass	Pass	Pass	Pass
14	3DS Spheres	Pass	Fail	Pass	Fail
15	Squeeze	Pass	Fail	Pass	Pass
16	Overlapping Sums	Fail	Pass	Pass	Pass
17	Runs	Pass	Fail	Pass	Pass
18	Craps	Pass	Pass	Pass	Pass

Table 8. The results of DIEHARD test in p-value pass rate $\geq$ 90% for rule 90, 150, and<90, 150> with PBCA(PB) & NBCA(NB) in 1-D

Test No.	Test Name	The results of tests (Pass or Fail)			
		U,PB	NU,PB	U,NB	NU, NB
1	Birthday Spacing	Pass	Pass	Pass	Pass
2	Over. 5-Per.	Pass	Pass	Pass	Pass
3	Binary Rank 31×31	Pass	Pass	Pass	Fail
4	Binary Rank 32×32	Pass	Pass	Fail	Fail
5	Binary Rank 6×8	Pass	Pass	Pass	Fail
6	Bitstream	Pass	Pass	Pass	Pass
7	OPSO	Pass	Pass	Pass	Pass
8	OQSO	Pass	Fail	Fail	Fail
9	DNA	Pass	Pass	Fail	Fail
10	Count-The-1's 01	Pass	Pass	Pass	Pass
11	Count-The-1's 02	Pass	Pass	Pass	Pass
12	Parking Lot	Pass	Pass	Pass	Pass
13	Minimum Distance	Pass	Pass	Pass	Pass
14	3DS Spheres	Pass	Fail	Pass	Fail
15	Squeeze	Pass	Pass	Pass	Pass
16	Overlapping Sums	Pass	Pass	Pass	Pass
17	Runs	Pass	Pass	Pass	Pass
18	Craps	Pass	Pass	Pass	Pass

Table 9. The results of DIEHARD test in p-value pass rate $\geq$ 90% for uniform(U) and nonuniform(NU) 2-D CA with PBCA(PB) & NBCA(NB)

Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (No. 2010-0011968).

8. References

Chowdhury, D. R., Subbarao, P. & Chaudhuri, P. P. (1993). Characterization of Two Dimensional Cellular Automata Using Matrix Algebra, *Information Sciences* 71: 289–314.

Guan, S.-U. & Tan, S. K. (Jul. 2004). Pseudorandom Number Generation With Self-Programmable Cellular Automata, *IEEE Transctions on Computer-Aided Design of Integrated Circuits and Systems* 23(7): 1095–1101.

Guan, S.-U. & Zhang, S. (Feb. 2003). An Evolutionary Approach to the Design of Controllable Cellular Automata Structure for Random Number Generatio, *IEEE Transctions on Evolutionary Computation* 7(1): 23–36.

Guan, S.-U., Zhang, S. & Quieta, M. T. R. (2004). 2-D Variation With Asymmetric Neighborship for Pseudorandom Number Generation, *IEEE Transaction on Computers* 23: 378–388.

Hortensius, P. D., Mcleod, R. D., Pries, W., Miller, D. M. & Card, H. C. (1989). Cellular automata-based pseudorandom number generators for built-in self-test, *IEEE Transaction Computer-Aided Design* 8: 842–859.

Marsaglia, G. (1998). DIEHARD Test suite, *http://www.stat.fsu.edu/pub/diehard* .

Quieta, M. T. R. & Guan, S.-U. (2005). Optimization of 2-D Lattice Cellular Automata for Pseudorandom Number Generation, *International Journal of Modern Physics* 16(3): 479–500.

Seredynski, F., Bouvry, P. & Zomaya, A. Y. (2004). Cellular automata computations and secret key cryptography, *Parallel Computing* 30: 753–766.

Steeb, W.-H. (2001). *The nonlinear workbook: chaos, fractals, cellular automata, neural networks, genetic algorithms, fuzzy logic : with C++, Java, Symbolic C++ and Reduce programs*, World Scientific Publishing Co. Pte. Ltd.

Tan, S. K. & Guan, S.-U. (2007). Evolving cellular automata to generate nonlinear sequences with desirable properties, *Applied Soft Computing* 7: 1131–1134.

Tomassini, M., Sipper, M. & Perrenoud, M. (2000). On the generation of high quality random numbers by two-dimensional cellular automata, *IEEE Transactions on Computers* 49(10): 1146–1151.

von Neumann, J. (1966). *The Theory of Self-Reproducing Automata*, A.W Burks, ed., Univ. of Illinois Press, Urbana and London.

Walker, J. (Oct., 1998). ENT Test suite, *http://www.fourmilab.ch/random/* .

Wolfram, S. (1983). Statistical mechanics of cellular automata, *Reviews of Modern Physics* 55(3): 601–644.

Wolfram, S. (1984). Computation theory of cellular automata, *Communications in Mathematical Physics* 96: 15–57.

Wolfram, S. (1986). *Theory and Applications of Cellular Automata: Including Selected Papers, 1983-1986*, World Scientific.

Xuelong, Z., Qianmu, L., Manwu, X. & Fengyu, L. (Oct. 2005). A Symmetric Cryptography based on Extended Cellular Automata, *Proceeding of 2005 IEEE International Conference on Systems, Man and Cybernetics* 1: 499–503.

Cellular Automata - Innovative Modelling for Science and Engineering

Edited by Dr. Alejandro Salcido

ISBN 978-953-307-172-5
Hard cover, 426 pages
Publisher InTech
Published online 11, April, 2011
Published in print edition April, 2011

Modelling and simulation are disciplines of major importance for science and engineering. There is no science without models, and simulation has nowadays become a very useful tool, sometimes unavoidable, for development of both science and engineering. The main attractive feature of cellular automata is that, in spite of their conceptual simplicity which allows an easiness of implementation for computer simulation, as a detailed and complete mathematical analysis in principle, they are able to exhibit a wide variety of amazingly complex behaviour. This feature of cellular automata has attracted the researchers' attention from a wide variety of divergent fields of the exact disciplines of science and engineering, but also of the social sciences, and sometimes beyond. The collective complex behaviour of numerous systems, which emerge from the interaction of a multitude of simple individuals, is being conveniently modelled and simulated with cellular automata for very different purposes. In this book, a number of innovative applications of cellular automata models in the fields of Quantum Computing, Materials Science, Cryptography and Coding, and Robotics and Image Processing are presented.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Sang-Ho Shin and Kee-Young Yoo (2011). An Improved PRNG Based on the Hybrid between One- and Two-Dimensional Cellular Automata, Cellular Automata - Innovative Modelling for Science and Engineering, Dr. Alejandro Salcido (Ed.), ISBN: 978-953-307-172-5, InTech, Available from: http://www.intechopen.com/books/cellular-automata-innovative-modelling-for-science-and-engineering/an-improved-prng-based-on-the-hybrid-between-one-and-two-dimensional-cellular-automata

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821