Novel Pseudorandom Number Generator Scheme Employing 3-Dimensional Cellular Automata

Murad Khan, Jamil Ahmad, Awais Ahmad, Syed Ismail Shah
Department of Computing and Technology, IQRA University Islamabad, Pakistan

***Abstract* - This research proposes a novel three dimensional cellular automata (3-D CA) scheme for pseudo random number generation which is highly secure than the two dimensional cellular automata (2-D CA). It removes security and boundary problems with the 2-D CA. The use of 1-D CA was very common in late 80s which was then improved with 2-D CA. Research literature shows that 2-D CA is suffering from security and boundary problems. The proposed scheme is implemented using C++ to test its performance against others similar systems using DIHARD and ENT standard test suites. Simulations are performed on 200 sets for both DIHARD and ENT. Simulation results show that the proposed scheme performs better than that of the older version especially in terms of security and boundary. In DIEHARD and ENT test the proposed scheme produces better success rate than older versions.**

Key words: **Pseudorandom number generation, cellular automata, DIEHARD, ENT.**

1. INTRODUCTION

Random numbers (RN) are widely used in different cryptographic applications like cryptography, computer simulations, Digital water marking, and GSM (Ahmad, 2009). Different mathematical tools are used to construct high class of PRNG. These PRNGs are expected to be capable of generating a sequence that must possess three properties, (i) Long period (ii) good statistical properties (iii) linear complexity. These three properties of PRNG are verifiable through statistical analyses. These statistical methods put together in DIEHARD Test Package and ENT Test suites. The attempts to construct a high speed PRNG have met only qualified success. The phenomenon has been bedeviling cryptographers during the past decade. It includes Linear Feedback Shift Register (LSFR), linear congruential Generation (LCG) and cellular automata (CA). During the past few years CA has been the focus of research in cryptography(Wolfram S. , 1986), (TOMASSINI, 1996). Different types of CA were employed for PRNG processes (S. Nandi, 1994), (Zhao Xuelong, 2005). The foremost amongst the types has been one-dimensional cellular automata (1-D CA). The 1-D CA has two neighboring cells. In 1-D CA, a single cell can be updated by taking XOR operation on left and right cell of the middle cell(Jun, 2010). The 1-D CA had many limitations which ranged between boundary and security.

To remove the boundary and security problem in 1-D CA, researchers introduced a technique with the increased dimensions, i.e. 2-D CA. (D. Roy Chowdhury, 1994). The 2-D CA exhibited reduced boundary problems and a long period of PRNG(Sheng-Uei Guan, 2004). The increase in dimension and enhancement in structure of cellular automata have shown improved performance(Marco Tomassini, 1999).

While implementing 3-D CA, the period of PRNG is increased as compared to 2-D CA. Our technique uses the model of 3-D CA with two power bit streams to control a dynamic rule selection with 3-D CA starting from a single cell. At each step, a cell is filled in if the total number of cells around it matches value specified by the rule number. A rule is a method through which a single cell is updated. We have examined different rules during the experiments. Rules 63, 127, 191, and 255 demonstrate improved domino effect. These rules use XOR and XNOR logics coupled with dual strategies. Simulations results have been carry out in C++ language to verify the proposed method.

2. LITERATURE SURVEY

Applications of RN are widely used in different fields of engineering like cryptography, computer simulations, Digital water marking and GSM. Most of the digital watermarking algorithms are based on PRNG. In digital watermarking, a watermark is the PRN bit stream. A highly secure PRN is needed to deploy it in the watermarking algorithm (Steghrarzadeh, 2006). Different cryptographic algorithms need to encrypt data with a secret Pseudo Random Number. This PRN can be computed by PRNG. Symmetric key encryption is widely used in

Proc. of the International Conference on Advances in Computing and Networking – ACN 2012
Edited by Dr. R. K. Singh.
Copyright © 2012 Universal Association of Computer and Electronics Engineers . All rights reserved.
ISBN: 978-981-07-2683-6

different scenarios. The session key for the symmetric encryption derives essence from PRNG (Fengyu, 2005). Different protocols use different cryptographic algorithms of communication. Cryptographic algorithms employ specific keys. The generation of these keys is vital. It can be produced through random numbers algorithm (E.Knuth, 1981). The sequence that is produced by mathematical method is instinctively deterministic. The RN can easily be broken by different cryptanalysis attacks. The generation of PRNG in itself is a complicated chore. Different algorithms have been proposed by different researchers. The first algorithm was suggested by John von Neumann, which is called middle-square method (Neumann, 1951). The said algorithm takes a number, calculates the square of that number, and then takes the middle number as a RN. Cryptographically secure PRNG have been proposed, these include stream ciphers, block cipher with CBC, and output feedback (Christophe Petit, 2008). The introduction of CA has also been proposed by different researchers [5], [7] and [8]. CA has shown some good results. The very first research on CA has been proposed by Wolfram(Wolfram S. , Statistical Mechanics of Cellular Automata, 1983). A mathematical model has been proposed for 1-D CA, where a cell is updated by its left and right cell. Wolfram suggests different rules for different structures of 1-D CA [2]. Depending upon the dimension of CA, a single cell is attached with its 'n' neighbors. A single cell can be updated accordingly to a fix rule i.e., 1-D CA. A single cell in 1-D CA can be updated by its left, right, and the updated cell itself. Hence this type of mechanism leads us to the construction of rules. Different rules of 1-D CA have been proposed by Wolfram [2].

Because of two major issues a 2-D CA has been introduced by Wolfram (Bhattacharyya, 2004). The structure of the 2-D CA is like a coordinate system, where every cell has its own location in the coordinate plane. The location of each cell is represented by the intersection of a row and a column. The address of the cell is represented by *(x, y)* in a 2-D plane—similar to a point in the coordinate plane.

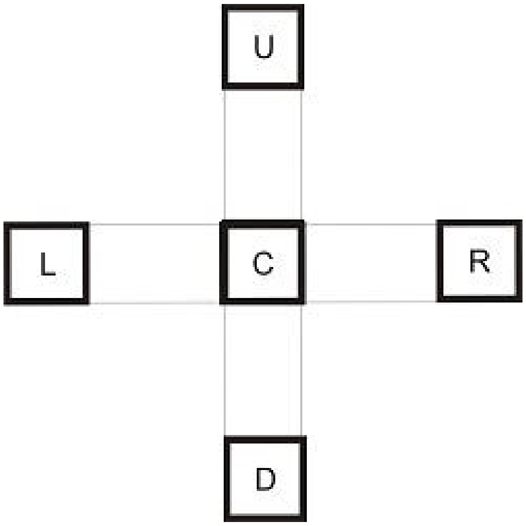

Figure 1: Structure of a 2D-CA Cell (**U** = Up cell **D** = Down cell **L**= Left cell **R** = Right Cell **C** = Center Cell)

On a single execution of the structure each cell in the structure is updated. This mechanism is monitored and controlled by a time variable. The time variable is incremented each time the structure gets executed. Each cell in the structure is updated according to a specific rule. The rule with good randomness can be achieved by running the algorithm on different instances of time. The rule that produces good random numbers is then saved. A state of a cell in the cellular automata is represented by $S_{(x,y)}$, and a state with some specific time is represented by involving a time variable with a state i-e $S_{x,y}(t)$. The present state is represented by $S_{x,y}(t)$ while the future state is represented by $S_{x,y}(t+1)$. Each time the structure is executed according to a specific rule the time variable is incremented by a value of one. In a single execution of the structure, each cell is updated and a bit stream is generated with a large period. Main problem with CA structure is its boundary problem. These boundary problems emanate in cellular automata because of the presence of extreme cells in the CA. During the executions of these cells overflow of bits stream occurs, which reduces the efficient statistical properties of a PRNG. To overcome such problem the mechanism of periodic boundary conditions has been proposed [7]. In this mechanism extreme cells are concatenated with adjacent cells. This type of boundary conditions has advantages over null boundary conditions where extreme cell is concatenated with logic 0-state [8]. The limitation in the periodic boundary conditions is its linear structure because of concatenating last column cells with the cells of first column. Hence a linear relationship produces in the structure. This limitation has been solved in the proposed solution where a property of

SEEK DIGITAL LIBRARY

block cipher called diffusion is introduced in the proposed structure.

3. RNG BASED ON 3-D CA

To overcome the security and boundary problems with 2-D CA a novel 3-D CA has been proposed in this paper. The structure proposed by this cellular automaton is highly secure. The results are shown in the end of this paper. The sequence generated by 3-D CA is very accurate and conveniently manageable. A good PRNG has three different properties: Large period, good statistical properties, and large linear complexity to achieve all of these properties, we introduce two bit streams that are power bit-stream 1 and 2. These bit-streams are capable of controlling the structure of proposed CA. The proposed boundary condition mechanism is able to generate random numbers with large period and good statistical properties. Our time swapping mechanism is able to generate random number with high period. The PRNG is then passed through ENT and DIEHARD test suite to test the randomness of PRNG. We tested different result of our proposed system and finally we got rule number 63, 127, 191 and 255. These rules produce much better results as compared to other rules. A rule is defined by 8-bits where 2-bits represent power bits 1 and 2.The state of a cell is updated by the following procedure.

$$S_{x,y,z}(t+1)=P_{bit1} \oplus P_{bit2} \oplus L\text{-}S_{x,y,z}(t) \oplus R\text{-}S_{x,y,z}(t) \oplus U\text{-}S_{x,y,z}(t) \oplus B\text{-}S_{x,y,z}(t) \oplus I\text{-}S_{x,y,z}(t) \oplus O\text{-}S_{x,y,z}(t)$$

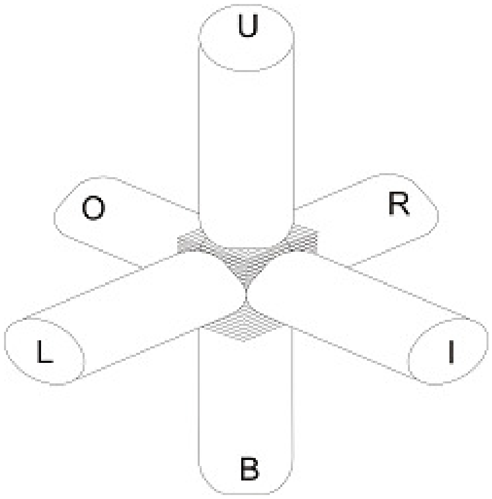

Figure 2: Structure of a 3D-CA Cell *(L=Left bit R=Right bit U=Upper bit B=Bottom bit I=In-page bit O=out-page bit)*

The power bit stream is used to control the rule applied. In our proposed system the Power bits stream 1 and 2 is fed with an initial vector *V1* and *V2* each of 512-bits using random sequence of 0s and 1s. All of the cells of 3-D CA are updated with a binary sequence of 1s and 0s. After a single execution the structure of 3-D CA is passed through the above algorithm which then generates 512 bits. These bits are stored in an output variable O-bit. The time swapping mechanism is then applied on O-bit block to achieve more randomness among different blocks of output bits.

Following algorithm is used in the proposed system:

Algorithm:
Input: pbit1, pbit2, arr[i][j][k].
Output: O-bit, time swapping mechanism
Basic Idea:

```
Loop i →0 to 512
        i ←rand( )%2
                Pbit1 ← i

Loop i →0 to 512
        i ← rand( )%2
                Pbit2 ← i
Loop i → 0 to 512
        i ← rand( )%2
                arr[i][j][k] ← i
Loop i → 0 to 8
        Loop j → 0 to 8
                Loop k → 0 to 8
                        O-bit ← arr[i][j][k]
                                Rule(O-bit)
```

In the start the 3-D PCA is first filled with 512 bits using rand() function. In a single execution the whole structure passes through a defined rule. The selection of the rule can be carried out through power bits used. The operation on a cell is shown in the following figure.

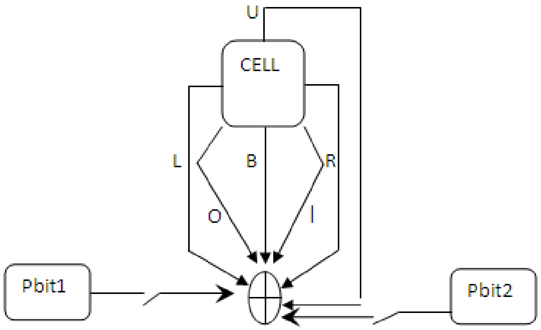

Figure 3: Structure of a 3D-PCA Cell

The selection of the rule is based on the injection of power bits. Following table shows the selection of rule.

SEEK DIGITAL LIBRARY

Table 1: Rules used in 3-D PCA

Rule	Pbit1	Pbit2	L	R	U	B	I	O
63	0	0	1	1	1	1	1	1
127	0	1	1	1	1	1	1	1
191	1	0	1	1	1	1	1	1
255	1	1	1	1	1	1	1	1

In the table it is shown that the rule used is governed by the power bits. The value of power bit dynamically changes during the program execution to control the structure of 3-D PCA and produces high randomness in the bits generated. During updating of the structure each cell is passes through a specific rule. The output stream is generated and stored in a vector array of specified length. The output that is generated is also passed to power bits sequence to keep the power bits sequence updated, and thus results a stream of bits with large period. This updation of the power bits sequence also keeps the rules in dynamic state, and hence the linear complexity among the generated bits is increased. The time swapping technique operates on different blocks and swap different blocks with each other. It randomly picks a block and then swaps it with another block randomly. This mechanism increases in good statistical properties of bits stream.

The time swapping mechanism operates as follows:

Initialize time_swap ( )

1. *Select O-bit block*$_i$
2. *Select O-bit block*$_j$
3. *Swap (O-bit block*$_i$*, O-bit block*$_j$*)*

Where i and j starts from 1 and ends on the requirements of the application. This mechanism runs until all of the output blocks end and swap all of the blocks with each other.

New boundary condition has been proposed. We name this new boundary condition as incremental boundary conditions. The last column in the system is concatenated with second column of *z* coordinate. By doing this we get diffusion in the system. This phenomenon of diffusion can increase the security of proposed system. We also check the coordinate of *x* and *y* but we found increase security in *z* coordinate.

4. EXPERIMENTAL RESULTS

Both the proposed 3-D CA and 2-D CA [17], [18] are implemented using same experimental environment such as ENT and DIEHARD test suites.

The DIEHARD tests comprise packages of different statistical tests. It includes 18 different tests. Every test has its own checking mechanism. A DIEHARD test suite is only intended to test generators not the file. The test is so powerful that it checks the randomness up to an extreme level. The test works on special format of data. The random bit sequence which is generated by a generator must convert to a format that is acceptable to DIEHARD. The test normally accepts random number in binary formats. DIEHARD test checks the random sequence more than 10 MB of size. If the size of the bits stream is less than 10 MB, DIEHARD will not accept it and will not shows the results. To achieve good results we pass an amount of sequence more than 10 MB. It checks the p-value of the random numbers. A pass is considered only if the p-value lies in the range $0.025<p<0.975$. We performed two hundred tests on our proposed system and then compared the average results with that of 2-D PCA. The ENT test suite consists of three different tests, Entropy, Chi-Square, and Serial correlation coefficient. The input to ENT is tested as bit stream of 8 bits at time and then it reflects the statistical properties of the bit stream. Following tables shows results from both 2-D CA and 3-D CA. we can see better improvements in case of 3-D CA.

Following table shows the average values of taken from both tests.

Table 2: Average from both Tests for 2D and 3D

Test	**2D**	**3D**
Entropy	7.9999	8.0000
chi-square	127.5026	127.5122
SCC	0.0002	0.0002
Birthday Swapping	0.5934	0.5999
Overlapping permutation	0.3699	0.3700
Binary rank 31 x 31	0.5709	0.5800
Binary rank 32 x 32	0.6356	0.6422
Binary rank 6 x 8	0.4095	0.5000
Bitstream	0.5092	0.6012
OPSO	0.5330	0.5300
OQSO	0.4988	0.5000
DNA	0.4971	0.5000
Count the ones 01	0.5860	0.5002
Count the ones 02	0.5309	0.5012
parking lot	0.4389	0.5003
Minimum Distance	0.5093	0.5959

SEEK DIGITAL LIBRARY

3DS Spheres	0.5120	0.6231
Squeeze	0.5136	0.5523
overlapping sum	0.5046	0.5900
Runs	0.5225	0.6232
Craps	0.5092	0.5452

The result of ENT test suite is shown in the following table:

Table 3: Test results of ENT test Suite

Test	**Highest position**
Chi-Square	Proximating 127.5
Serial correlation coefficient	Proximating 0.0
Entropy	8.0

The following figure shows the successful test rate, comparing the results of 2-D and 3-D:

Table 3: successful test rate for DIEHARD test suite

Test	**2D**	**3D**
Birthday swapping	100%	100%
Overlapping permutation	75%	80%
Binary rank 31 x 31	100%	100%
Binary rank 32 x 32	96%	98%
Binary rank 6 x 8	96%	98%
Bitstream	100%	100%
OPSO	100%	100%
OQSO	100%	100%
DNA	100%	100%
Count the ones 01	96%	94%
Count the ones 02	100%	96%
parking lot	100%	100%
Minimum Distance	99%	100%
3DS Spheres	98%	100%
Squeeze	94%	98%
overlapping sum	96%	100%
Runs	93%	98%
Craps	89%	92%

5. CONCLUSIONS

We have proposed a new 3-D CA based PRNG with enhance capability of producing PRNs with long period, good statistical properties and large linear complexity. The new boundary conditions mechanism shows better results against periodic boundary conditions. This new boundary conditions is able to maintain the structure of CA and give good quality random numbers with augmented period. The use of power bits to control the dynamicity of the rules increases the linear complexity in the output blocks. The updating of the power bit sequence with output bits increases the security of the rule used. The technique of swapping output blocks decreases the autocorrelations among different blocks.

The proposed mechanism is then tested on well known DIEHARD and ENT tests and it shows better performance against already known algorithms. The quality of proposed system is shown by the test results in section 4. The ENT test suite produces an almost 100% result which shows the eminence of our proposed system. The statistical package in DIEHARD test also shows better performance against known algorithms.

The improve results shown by our proposed system and the production of random numbers with long period proves our proposed system be the quality PRNG with enhance new boundary conditions. Finally we intimate our proposed 3-D CA will be competently employable in different cryptographic applications and computer simulations experiments.

References

[1] M. I. Ahmad, "Enhanced A5/1 cipher with improved linear complexity," in *Multimedia, Signal Processing and Communication Technologies, 2009. IMPACT '09. International*, Aligarh, 2009, p. 265.

[2] S. Wolfram, "Random sequence generation by cellular automata," *Advances in Applied Mathematics*, vol. 7, no. 2, pp. 123-169, Jun 1986.

[3] M. SIPPER and M. TOMASSINI, "Generating parallel random number generators by cellular programming," *International Journal of Modern Physics*, vol. 7, no. 2, pp. 181-190, sep 1996.

[4] B.K Kar and P Pal Chaudhuri S. Nandi, "Theory and applications of cellular automata in cryptography," *IEEE Transactions on Computers*, vol. 43, no. 12, pp. 1346-1357, Dec 1994.

[5] L. Qianmu, X. Manwu and L. F. Z. Xuelong, "A symmetric cryptography based on extended cellular automata," in *IEEE International Conference on Systems, Man and Cybernetics*, Hawaii, USA, 2005, pp. 499 - 503.

[6] D. Jun, L. Na, G. Yixiong and Y. Jun, "A High-performance Pseudo-random Number Generator Based on FPGA," in *International Conference on Wireless Networks and Information Systems, 2009. WNIS '09.* , Shanghai, 2010, p.

SEEK DIGITAL LIBRARY

290.

[7] I. Sengupta, and P. Pal Chaudhuri D. Roy Chowdhury, "A Class of Two-dimensional Cellular Automata and Their Applications in Random Pattern Testing," *JOURNAL OF ELECTRONIC TESTING*, vol. 5, no. 1, pp. 67-82, 1994.

[8] S. Zhang, Quieta, M.T and S.U.Guan, "2-D CA variation with asymmetric neighborship for pseudorandom number generation," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 23, no. 3, pp. 378 - 388, March 2004.

[9] M. Sipper, M. Zolla, and M.P.M. Tomassini, "Generating high-quality random numbers in parallel by cellular automata," *Future Generation Computer Systems*, vol. 16, no. 2-3, pp. 291-305, Dec 1999.

[10] K. Gheneh and V. Steghrarzadeh, "Secure Video Watermarking using Random Statistics and Combinatorial Optimization," in *2nd International Conference on Information & Communication Technologies, 2006*, Damascus, 2006, p. 1841.

[11] Z. Xuelong, L. Qianmu X. Manwu L. Fengyu, "A symmetric cryptography based on extended cellular automata," in *IEEE International Conference on Systems, Man and Cybernetics, 2005*, 2005, p. 499.

[12] Donald E.Knuth, *Seminumerical algorithms*, 2nd ed. Massachusetts, USA: Addison-Wesley, 1981.

[13] John von Neumann, "Various techniques used in connection with random digits," in *National Bureau of Standards Applied Mathematics Series*, Washington, D.C, U.S, 1951, pp. 36-38.

[14] F-X. Standaert, O. Pereira, T. G. Malkin and M. Y. C. Petit, "A block cipher based pseudo random number generator secure against side-channel key recovery," in *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, New York, USA, 2008.

[15] S. Wolfram, "Statistical Mechanics of Cellular Automata," *Review of Modern Physics*, vol. 55, pp. 601-644, 1983.

[16] P Bhattacharyya. (2004, Apr) Cellular Automata: Wolfram's Metaphors for Complex Systems.

[17] D-H. Lee and C-P. Hong and B-H. Kang, "High-Performance Pseudorandom Number Generator Using Two-Dimensional Cellular Automata," in *4th IEEE International Symposium on Electronic Design, Test and Applications, 2008*, Hong Kong, 2008, pp. 597 - 602.

[18] S-U. Guan and S. Zhang, "An evolutionary approach to the design of controllable cellular automata structure for random number generation," *IEEE Transactions on Evolutionary Computation,* , vol. 7, no. 1, p. 23, February 2003.

SEEK
DIGITAL LIBRARY