iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** Issue- III **Month of publication:** November 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Special Issue-3, November 2014
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Design and Implementation of Pseudo Random Number Generator Used in AES Algorithm

N.Madhavi [1], R.Viswanadham[2]
M. Tech Student, Department of ECE, Shri Vishnu Engg College for women
Asst. Professor, Department of ECE, Shri Vishnu Engg College for women

Abstract: This paper presents a new Design for the generation of advanced encryption of (bit) data. The Design opted to obtain this encrypted data is RM-PRNG. This design also enhances the statistical properties of a chaos-based logistic map pseudo random number generator (PRNG) and extends the system period length. The reseeding method removes the short periods of the digitized logistic map and the mixing method extends the system period length to by "XOring" with a DX generator. This design also attains the throughput rate of 6.4 GB/s. The mixing method extends the system period length by Xoring with ALG and the reseeding method removes the short periods which are occurred by CB-PRNG
Index Terms- pseudo random number generator (PRNG), reseeding, Linear Congruential Generator (LCG), Carry-Look ahead Adder (CLA), Gate Equivalent (GE).

I. INTRODUCTION

Pseudo random number generator (PRNG) is an algorithm for generating a sequence generator. PRNG has been widely find applications in Monte carlo generation, telecommunication systems, test pattern generation.

A good PRNG should have characteristics of

1) Long-period random number sequence

2) Fit in statistical properties

3) A high throughput rate

4) Unpredictability

Linear PRNGs, such as linear feedback shift registers (LFSRs), linear congruential generators (LCGs), and multiple re- cursive generators (MRGs) can produce long-period random number sequences. Linear PRNGs when implemented gives efficient throughput rate and hardware cost, but the output of such Prng's can be predictable due to the linear structure. Someone linear PRNGs in dealt with the predictability problem but incurred higher hardware cost and more process time . To overcome that predictability problem non linear chaos-based PRNG (CB-PRNG) is proposed. we propose a reseeding-mixing PRNG (RM-PRNG) that consists of a CB-PRNG and a long-period MRG. The reseeding method removes the disadvantages of short periods in CB-PRNG while the mixing of the CB-PRNG with an MRG pushes the overall system period length to a value ($> 2^{253}$ in 32-b implementation) based on simple theoretical calculation. By outputting multiple bits per iteration high throughput rate of (6.4 Gb/s) is achieved. So there is a need to implement a design which produces long periods and high throughput rate. Thus RM-PRNG is proposed.

II. EXISTING SYSTEM

In general, mixing multiple CB-PRNGs results in higher hardware cost, lower throughput rate, and longer but unpredictable period length. Furthermore, one cannot be sure that the random numbers produced by these mixed PRNGs will have acceptable statistical properties. Since higher hardware cost is due to implementation of multiple CB-PRNG switch are more complex than linear

Special Issue-3, November 2014
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

PRNGs, mixing a CB-PRNG with a linear MRG instead of mixing two CB-PRNGs will reduced the hardware cost.

A. *Existing System Drawbacks*

- Hardware cost.
- Lower Throughput Rate
- unpredictable period length
- It's not sure that the random numbers produced by these mixed PRNGs will have acceptable statistical properties.

III. PROPOSED DESIGN (RM-PRNG)

In our proposed RM-PRNG, which consists of a CB-PRNG and an MRG, the period length is considerably extended because the period length of the MRG is much longer than that of the CB-PRNG while the short periods of the CB-PRNG can be removed by our reseeding algorithm. We can analytically calculate the lower bound of the period length in RM-PRNG in terms of the period length of the CB-PRNG and that of the MRG. The enhancement of throughput rate is achieved by using a vector-mixing technique in the proposed RM-PRNG. As the linear structure of the MRGs is broken by mixing with a CB-PRNG, the statistical properties will get improved.

IV. DESIGN APPROACH

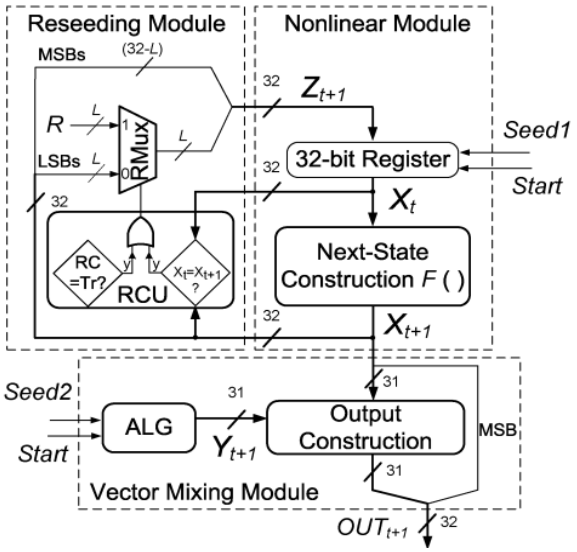


Fig.1 Structure of the proposed RM-PRNG

RM-PRNG is composed of three modules: Non linear module, Reseeding module, Vector mixing module. In a 32-b implementation, the Nonlinear Module has a controlled 32-b state register and a Next- state construction circuitry. The controlled register stores the state value Xi which can be set to seed 1 by the start command. The Next - state construction circuitry produces the next state value according to the recursive formula. For each state value generated, the reseeding control unit (RCU) in the Reseeding Module compares the values of and for checking the fixed point condition and increases the reseeding counter (RC) at the same time. The RC will be reset and the reseeding operation will be activated when either the fixed point condition is detected or the RC reaches the reseeding period.

Special Issue-3, November 2014
ISSN: 2321-9653

A. Nonlinear Module

For Next state construction, LCM is used in the Non linear Module so that

$$X_{t+1} = F(X_t) = \gamma X_t(1 - X_t), \quad t \geq 0$$

with $\gamma = 4$ and $X_0 \in (0, 1)$ as an initial seed. Choosing a value 4 for γ not only makes the LGM chaotic but also simplifies the implementation of equation to merely left-shifting the product of Xt and 1-Xt by 2 b. The state size decreases from 32 to 31 b, as the dynamics and in the equation are the same. This is equivalent to a degradation of resolution by 1 b. In addition, fixed points (at X_t=0 and 0.75) as well as short periods exist when the LGM is digitized. From exhaustive runs for all of the seeds, we obtain all other periods for the 32-b LGM without reseeding. The performance of a CB-PRNG using only the Nonlinear Module is unsatisfactory. So, to solve the fixed points and short-period problem, a new Reseeding Module is in proposed.

B. Reseeding Module

Reseeding mechanism is obvious for the removal of the fixed points. When the reseeding period is reached or fixed point condition is detected, the value Zt+1 loaded to the state register will be perturbed away from Xt+1 in the RCU by the fixed pattern according to the formula

$$Z_{t+1} = \begin{cases} X_{t+1}[j], & 1 \leq j \leq 32 - L; \\ R[i], & 33 - L \leq j \leq 32, \ i = j + L - 32 \end{cases}$$

Where subscripts i,j are the bit-index L is integer, and $R \neq 0$. Degradation of the statistical properties of chaos dynamics can be minimized by making the magnitude of the perturbation of the fixed pattern R small compared with X_t. Here, we set L=5 so that the maximum relative perturbation is only $(2^5 - 1)/2^{32}$ and the degradation can be ignored. The effectiveness in the removal of short periods depends on the reseeding pattern R and the reseeding period T_r. for suitable combination of T_r and R. First, the reseeding period should avoid being the values or the multiples of the short periods T_s of the unperturbed digitized LGM. Otherwise, if the 5 LSBs of X_{t+1} equal to R when the reseeding procedure is activated, Z_{t+1} will be equal to X_{t+1}. Then no effective reseeding will be realized and the system will be trapped in the short period cycle. Hence, prime numbers should be used as the reseeding period candidate.

C. Vector Mixing Module

The DX generator which is an efficient MRG serves as the ALG in Vector Mixing Module. Specifically, we choose the DX generator with the following recurrence equation:

$$Y_{t+1} = Y_t + B_{DX} \cdot Y_{t-7} \mod M, \quad t >= 7$$

Using an efficient search algorithm [8], we find that the particular choice of $B_{DX} = 2^{28}+28$ and M=231-1 gives the maximum period of the DX generator. The LSBs of Yt+1 and that of Xt+1 are mixed in the Output Construction unit using a XOR operation to obtain the least significant bits of the output according to the equation

$$OUT_{t+1}[1:31] = X_{t+1}[1:31] \text{ (ex-or) } Y_{t+1}[1:31]$$

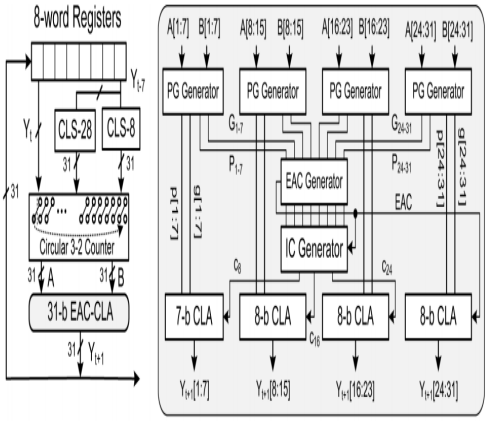
Then, the most significant bit (MSB) of Xt+1 is attached to OUTt+1 [1:31] to form the full 32-b output vector OUTt+1.

1) DX Generator

DX generator implementation is (the ALG) done by using 8-word registers, circular-left-shift (CLS), circular 3-2 counter and End Around Carry- carry look ahead adder (EAC-CLA). By using flip-flops the eight-word register was implemented. For generating

Special Issue-3, November 2014
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

two partial products signal Yt-7 is circular-left-shifted 28 and 8 b, using the modules CLS-28 and CLS-8 respectively. To combine these three 31-b operands into two 31-b operands a circular 3-2 counter is used, which consumes 247 gates. To evaluate Y_{t+1} 31-b EAC-CLA is used with 348 gates. The schematic design of the 31-b EAC-CLA [4], [9] is shown in the below Figure. The schematic design of the 31-b EAC-CLA includes four modules they are propagation and generation (PG) generators, end-around-carry (EAC) generator, internal carry (IC) generator, and CLAs .When EAC is generated by group of PGs, EAC is then fed to the IC generator and then to least-significant 8-b CLA. On CLAs, the final addition was performed.



(a) (b)

Fig.2 (a) Structure of the DX generator

(b) Structure of the 31-b EAC-CLA

V. DIGITIZATION

Digitization is the process of converting information into a digital format . In this format, information is organized into discrete units of data (called bit s) that can be separately addressed (usually in multiple-bit groups called byte s). This is the binary data that computers and many devices with computing capacity (such as digital camera s and digital hearing aid s) can process.

Text and images can be digitized similarly: a scanner captures an image (which may be an image of text) and converts it to an image file, such as a bitmap . An optical character recognition (OCR) program analyzes a text image for light and dark areas in order to identify each alphabetic letter or numeric digit, and converts each character into an ASCII code.

we make digitization of the logistic map as follows: Firstly, the chaotic sequence is generated through Equations, which has to be amplified by a scaling factor (10^4) and round to integer-sequence according to Equations

$$Z_k=\text{round}((x_k * 10^4) \bmod 256)$$

This transformation implies that, when the randomly generated chaotic sequence (input values) is uniformly distributed, the output of the digitization process is also uniformly distributed Random numbers have been used extensively in many simulation applications like Monte Carlo Integration or computer modeling. But recently security applications have increased the need for strong (secure) random number generation like automatic password generation, encryption algorithms, on-line gambling etc. Thus random number generation has become a challenging and an interesting task. Most classical random number generators, generate sequences that are either linear or predictable hence not suitable for cryptographic and security applications. Others generate

sequences that even though they are secure they are not cryptographically strong and above all are slow in execution. Also recent advances in random number generation like the construction of Multiple Recursive Generator (MRG) with large orders, Fast Multiple Recursive.

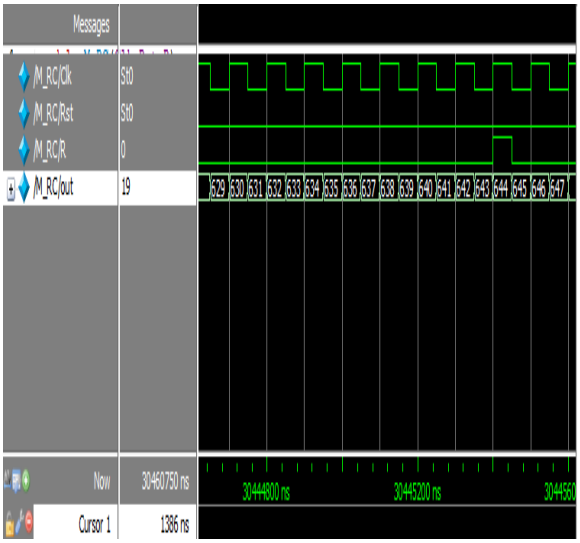
Generator (FMRG) and DX (system of multiple recursive generators proposed by Deng and Xu generators does not generate a strong random number sequences. Though MRGs have extremely long period of length with good empirical performance, its recurrence equation can be solved given a small set of its generated sequence, this implies that MRGs and FMRGs are not strong cryptographic generators. We propose an algorithm that will transform linear sequences generated by both classical LCG, MRGs, FMRGs and DX generators and make them cryptographically strong generators by hiding the entire sequence generated by the generators, thus it will be difficult for cryptanalyst to predict or infer the generator sequence if even the partial sequence or the parameters or knowledge of the algorithm used in the transformation of the generators are known Experimental results and tests have shown that classical generators like LCGs that generate pseudorandom linear sequences are not suitable for cryptographic purposes, even though it is simple, efficient and easy to generate. Other classical generators like BBS, RSA, and BM etc that are thought to be secure are equally not good enough for cryptographic purposes as they are slow in generating the next random bit sequence. Also the recent advances in random number generation (MRGs and FMRGs) are fast and efficient in generating linear sequences with long periods and good empirical performance, but still they are not cryptographically strong as the linear system can be predicated using a system of unique k equations. Our proposed algorithm produces a strong pseudorandom sequence that is suitable for cryptographic purposes and difficult to predict/infer by transforming the linear sequences and breaking its linear structure. The transformation hides the linear bits of the generated linear sequence preventing the attacker from accessing the generated output sequence, even with the knowledge of the partial sequence, parameters of the generators and the algorithm used in transforming the generator sequence. Thus knowing the parameters and partial sequence of the generators does not pose any threat any longer as the prediction of the generator sequence will no longer be an easy one.

Proposed System Advantages:

- High Throughput Rate
- Less hardware cost

VI. SIMULATION RESULTS

RC (Reseeding counter)



Special Issue-3, November 2014
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

FINAL OUTPUT (Random number sequence)

VII. CONCLUSION

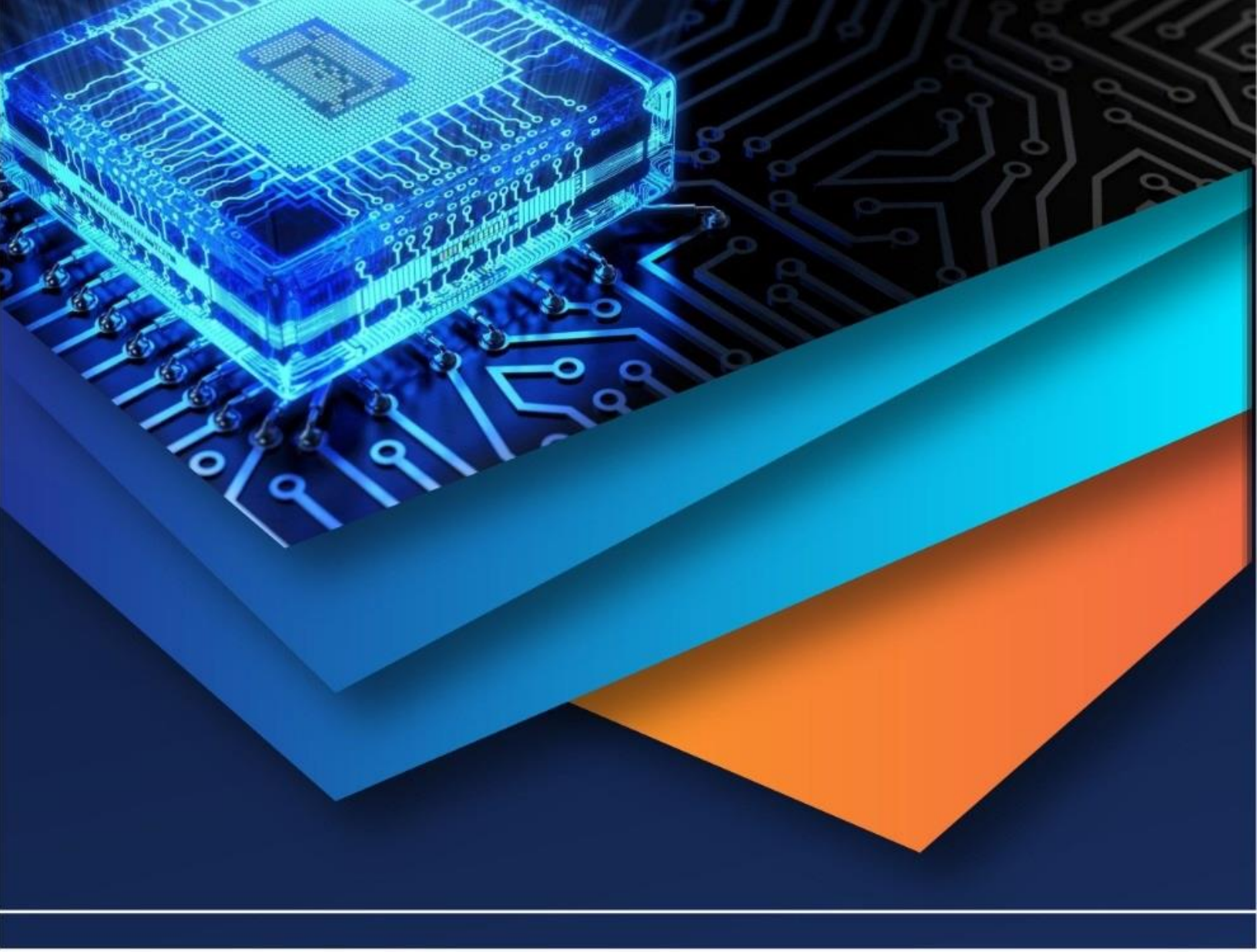
The proposed reseeding mechanism solves the short-period problem originated from the digitization of the chaotic map. The long-period DX generator extends the period length to the theoretically calculated value greater than 2^{253} when it is get mixed with the CB_PRNG . Replacing a hardware-demanding CB-PRNG with a hardware-efficient MRG, the hardware cost is reduced and the hardware efficiency achieves 0.538 Mb/s-gate. Due to the generation of multiple random bits in an iteration by the RM-PRNG, the high throughput rate (> 6.4 Gb/s) is attained. By improving the statiscal properties of the reseeding method the randomness will be enhanced. The generated random number sequences by the proposed RM-PRNG pass all the tests in NIST SP 800-22 test suite. Because of these benefits the proposed nonlinear RMPRNG can serve as a good technique in the cryptographic applications and telecommunication.

VIII. FUTURE SCOPE

Reseeding-Mixing method, proposed design supports higher throughput and lower hardware cost and generates a unpredictable random number sequence. So, that sequence can be used as a secret key in encryption and decryption circuits.

REFERENCES

[1] J. E. Gentle, Random Number Generation and Monte Carlo Methods, 2nd ed. New York: SpringerVerlag, 2003.
[2] M. P. Kennedy, R. Rovatti, and G. Setti, Chaotic Electronics in Telecommunications. Boca Raton, FL: CRC, 2000.
[3] D. Knuth, The Art of Computer Programming, 2nd ed. Reading, MA: Addison-Wesley, 1981.
[4] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," J. Cryptology, vol. 10, pp. 111–147, 1997.
[5] D. H. Lehmer, "Mathematical methods in largescale computing units," in Proc. 2nd Symp. Large Scale Digital Comput. Machinery, Cambridge, MA, 1951, pp. 141–146, Harvard Univ. Press.
[6] P. C. Wu, "Multiplicative, congruential randomnumber generators with multiplier and modulus ," ACM Trans. Math. Software, vol. 23, pp. 255–265, 1997.
[7] L. Y. Deng and H. Xu, "A system of highdimensional, efficient, longcycle and portable uniform random number generators," ACM Trans.ModelComput. Simul., vol. 13, no. 4, pp. 299–309, Oct. 1, 2003.
[8] L. Y. Deng, "Efficient and portable multiple recursive generators of large order," ACM Trans. Modeling Comput. Simul., vol. 15, no. 1, pp. 1–13, Jan. 2005.
[9] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo- random number generator," SIAM J. Comput., vol. 15, pp. 364–383, 1986.
[10] B. M. Gammel, R. Goettfert, and O. Kniffler, "An NLFSR-based stream cipher," in Proc. IEEE Int. Symp. Circuits Syst., 2006, pp. 2917–2920.
[11]D.Mukhopadhyay,D.R.Chowdhury,andC.Rebeiro,"Theory of composing non-linear machines with predictable cyclic structures,"inProc. 8th Int. Conf. Cellular Autom. Res. Ind., 2008, pp. 210–219, Springer.
[12]D.Mukhopadhyay,"Grouppropertiesofnonlinearcellularautomata," J. Cellular Autom., vol. 5, no. 1, pp. 139–155, Oct. 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY