2 Dimensional Cellular Automata Based Design of Private Key Encryption Algorithm

[1]N.Vigneshwaran, [2]K.J.Jegadishkumar,
[1]PG Scholar, [2]Assistant Professor,
[1]ECE, SSN College Of Engineering, Kaalavakam, India
[2]ECE, SSN College Of Engineering, Kaalavakam, India
[1]vignesh.1088@gmail.com, [2]jegadishkj@ssn.edu.in

***Abstract*— This paper presents the design of a Private key Algorithm based on 2-Dimensional Cellular Automata. Initial implementation of the Stream cipher is done using matlab tool to analyze its functionality and security. Advancement in computing technology applications like mobile communication, PDAs, navigational devices are at present being a part of everyone life. But these devices are restricted in computational power consumption, memory storage and data rate. Needs Security services like Confidentiality, Data integrity, and Authentication.**

***Index Terms*— Cryptography, key, Stream Cipher, Cellular Automata, CA Rules, Von Neumann Functionality**

I. INTRODUCTION

Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient plaintext ciphertext plaintext encryption decryption. Cryptography is the science of securing data, cryptanalysis the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

A key is a value that works with a cryptographic algorithm to produce a specific ciphertext. Keys are basically really, really, really big numbers. Key size is measured in bits; the number representing a 1024-bit key is darn huge.In public key cryptography, the bigger the key, the more secure the ciphertext. However, public key size and conventional cryptography's secret key size are totally unrelated. A conventional 80-bit key has the equivalent strength of a 1024-bit public key. A conventional 128-bit key is equivalent to a 3000-bit public key. Again, the bigger the key, the more secure, but the algorithms used for each type of cryptography are very different and thus comparison is like that of apples to oranges. Encrypted ciphertext encrypted message session key recipient's private key used to decrypt session key session key used to decrypt ciphertext original plaintext.

Cellular Automata

A cellular automation (CA) is a discrete model studied in computability theory, mathematics, physics, complexity science, theoretical\ biology and microstructure modeling. Cellular automata are also called cellular spaces, tessellation automata, homogeneous structures, cellular structures, tessellation structures, and iterative arrays.

A cellular automaton consists of a regular grid of cells, each in one of a finite number of states, such as on and off (in contrast to a coupled map lattice). The grid can be in any finite number of dimensions. For each cell, a set of cells called its neighborhood is defined relative to the specified cell. An initial state (time t=0) is selected by assigning a state for each cell. A new generation is created (advancing t by 1), according to some fixed rule (generally, a mathematical function) that determines the new state of each cell in terms of the current state of the cell and the states of the cells in its neighborhood. Typically, the rule for updating the state of cells is the same for each cell and does not change over time, and is applied to the whole grid simultaneously, though exceptions are known, such as the stochastic cellular automaton and asynchronous cellular automation.

One Dimensional Cellular Automata

Two Dimensional Cellular Automata

One Dimensional Cellular Automata

The simplest nontrivial CA would be one-dimensional, with two possible states per cell, and a cell's neighbors' defined to be the adjacent cells on either side of it. A cell and its two neighbors' form a neighborhood of 3 cells, so there are 2^3=8 possible patterns for a neighborhood. A rule consists of deciding, for each pattern, whether the cell will be a 1 or a 0 in the next generation.

There are then 2^8=256 possible rules [3]. These 256 CAs are generally referred to by their Wolfram code, a standard naming convention invented by Wolfram that gives each rule a number from 0 to 255. A number of papers have analyzed and compared these 256 CAs. The rule 30 and rule 110 CAs are particularly interesting. The images below show the history of each when the starting configuration consists of a 1 (at the top of each image) surrounded by 0's. Each row of pixels represents a generation in the history of the automaton, with t=0 being the top row. Each pixel is colored white for 0 and black for 1.

Rule 30 exhibits class3 behaviour, meaning even simple input patterns such as that shown lead to chaotic, seemingly random histories.

Rule 110, like the Game of Life, exhibits what Wolfram calls class 4 behaviour, which is neither completely random nor completely repetitive. Localized structures appear and interact in various complicated-looking ways. In the course of the development of a new kind of science, as a research assistant to Wolfram in 1994, Matthew Cook proved that some of these structures were rich enough to support universality. This result is interesting because rule 110 is an extremely simple one-dimensional system, and one which is difficult to engineer to perform specific behaviour.

Two- Dimensional Cellular Automata

Von Neumann Neighborhood

In cellular automata, the Von Neumann neighborhood comprises the four cells orthogonally surrounding a central cell on a two-dimensional square lattice. The neighborhood is named after John von Neumann, who used it for his pioneering cellular automata including the Universal Constructor. It is one of the two most commonly used neighborhood types, the other one being the 8-cell Moore neighborhood. It is similar to the notion of 4-connectedpixels in computer graphics. The concept can be extended to higher dimensions, for example forming a 6-cell octahedral neighborhood for a cubic cellular automaton in three dimensions. The von Neumann neighborhood of a point is the set of points at a Manhattan distance of 1.

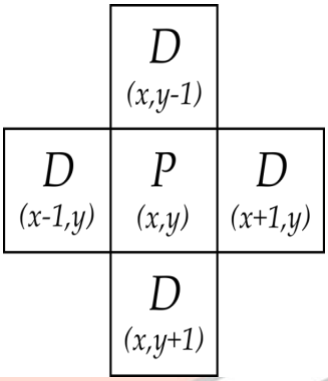

Fig 1. Two Dimensional 5 state Von Neumann neighborhood

Transmission state rules

The flow of bits between cells is indicated by the direction property. The following rules apply:

- Transmission states apply the OR operator to inputs, meaning a cell in a transmission state (ordinary or special) will be excited at time **t+1** if *any* of the inputs pointing to it is excited at time **t**
- Data passes from cells in the ordinary transmission states to other cells in the ordinary transmission states, according to the direction property (in the cell's direction only)
- Data passes from cells in the special transmission states to other cells in the special transmission states, according to the direction property (in the cell's direction only)
- The two subsets of transmission states, ordinary and special, are mutually antagonistic: Given a cell **A** at time **t** in the excited ordinary transmission state pointing to a cell **B** in any special transmission state at time **t+1** cell **B** will become the ground state. The special transmission cell has been "destroyed.". A similar sequence will occur in the case of a cell in the special transmission state "pointing" to a cell in the ordinary transmission state

Rule 30 CA function

Rule 30 is a one-dimensional binary cellular automaton rule introduced by Stephen Wolfram in 1983. Wolfram describes it as being his "all-time favourite rule" and details it in his book, A New Kind of Science. Using Wolfram's classification scheme, Rule 30 is a Class III rule, displaying aperiodic, chaotic behavior.

This rule is of particular interest because it produces complex, seemingly random patterns from simple, well-defined rules. Because of this, Wolfram believes that Rule 30, and cellular automata in general, are the key to understanding how simple rules produce complex structures and behavior in nature. Rule 30 has also been used as a random number generator in Wolfram's program Mathematic, and has also been proposed as a possible stream cipher for use in cryptography.

The evaluated function for RCA rule 30 is

$$x_i(t+1) = \left[x_i(t) \vee x_{i+1}(t) \oplus x_{i-1}(t)\right] \oplus x_i(t-1) \quad \textbf{(1)}$$

$$x_i(t-1) = \left[x_i(t) \vee x_{i+1}(t) \oplus x_{i-1}(t)\right] \oplus x_i(t+1) \quad \textbf{(2)}$$

Rule 45 CA function

For Rule 45, the rule set which governs the next state of the automaton is:

The evaluated function for CA rule 45 is

$$x_i(t+1) = \left[x_i(t) \vee (\bar{x}_{i+1}(t)) \oplus x_{i-1}(t)\right] \oplus x_i(t-1) \quad \textbf{(3)}$$

$$x_i(t-1) = \left[x_i(t) \vee (\bar{x}_{i+1}(t)) \oplus x_{i-1}(t)\right] \oplus x_i(t+1) \quad \textbf{(4)}$$

Stream Cipher

Stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (key stream). In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the key stream, to give a digit of the cipher text stream. An alternative name is a state cipher, as the encryption of each digit is dependent on the current state. In practice, a digit is typically a bit and the combining operation an exclusive-or (xor).

The pseudorandom key stream is typically generated serially from a random seed value using digital shift registers. The seed value serves as the cryptographic key for decrypting the cipher text stream.

Stream ciphers represent a different approach to symmetric encryption from block ciphers. Block ciphers operate on large blocks of digits with a fixed, unvarying transformation. This distinction is not always clear-cut: in some modes of operation, a block cipher primitive is used in such a way that it acts effectively as a stream cipher. Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity. However, stream ciphers can be susceptible to serious security problems if used incorrectly (see stream cipher attacks

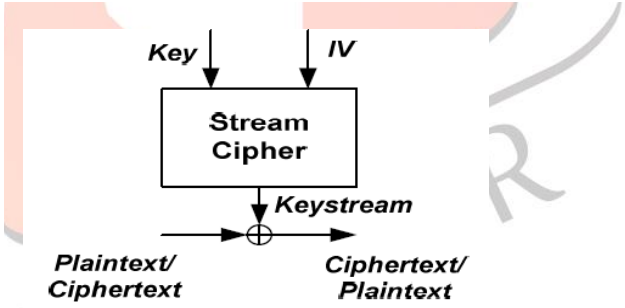

Fig. 2 Block diagram of stream cipher

II. DESIGN ALGORITHM METHODOLOGY

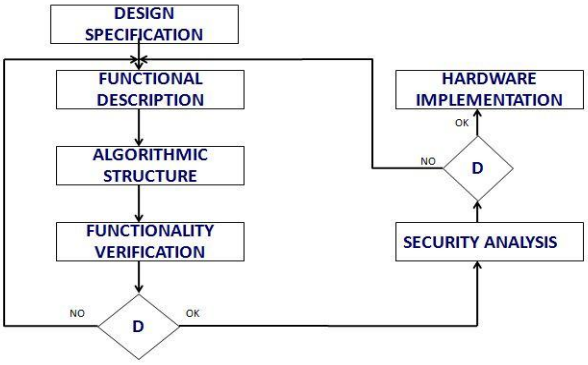

Fig 3. Block Diagram of Design Methodology

Proposed Algorithmic Structure

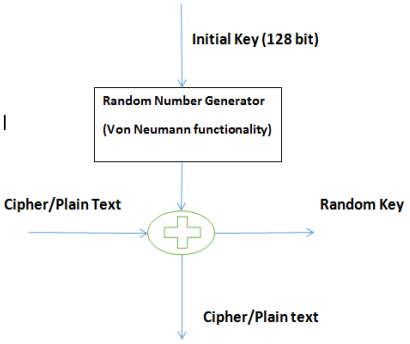

Fig 4. Block diagram of Algorithmic Structure

DESIGN SPECIFICATIONS

The proposed algorithmic structure is basically a stream cipher which works on 128 bit random input and 128 bit initial key in a one dimensional data. Then the one dimensional data bits are converted into matrix format, in two dimensional data format. The figure shows the basic structure of the Stream cipher. Here the Von Neumann functionality has used to generate the random number. Then the plain text is converted into cipher text with the generated random number key.

III. DESIGN AND SIMULATION RESULTS

DESIGN TEST CRITERIA

A) Non Linearity Test

Let, f is a Boolean function of variables, x1; x2; : : : xn and 'A' be the set of all affine functions in x1; x2; : : : xn. The minimum of the Hamming distances between f and the Boolean functions in A is the nonlinearity of function f.

B) Autocorrelation

The test performs the autocorrelation of the sequence and compares the value of the Maximum peak with the value in the origin. The worst result of this test is when there is a large peak because many of bits shifted will reflect the same behaviors as the originals. It is preferably having many reasonable middle peaks than the few high peaks, also due to the correlation immune attack.

C) Balanced Property

Balance (regularity) is another important criterion which should be fulfilled by a Boolean function used in ciphering [10]. This means that each output bit (0 or 1) should appear an equally number of times for all possible values of inputs. The balance of a Boolean function is measured using its Hamming Weight and is defined as:

Boolean function is balanced when its Hamming Weight is equal to $2n-1$.

D) Frequency Test

The focus of the test is the proportion of zeroes and ones for the entire sequence. The purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to ½ that is, the number of ones and zeroes in a sequence should be about the same. All subsequent tests depend on the passing of this test.

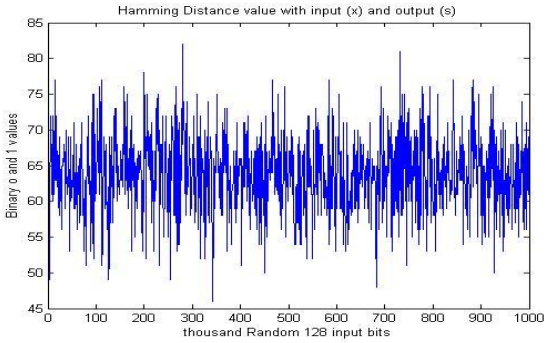

Fig 5. Hamming Distance value

Fig 5 shows the 68% hamming distance, then most of the values are in the center region and the values are equally distributed in the graph. The Hamming distance between two strings of equal length is the number of positions at which the corresponding symbols are different. So for 128 bit input almost 50% of the values of zeros and ones are evenly distributed.

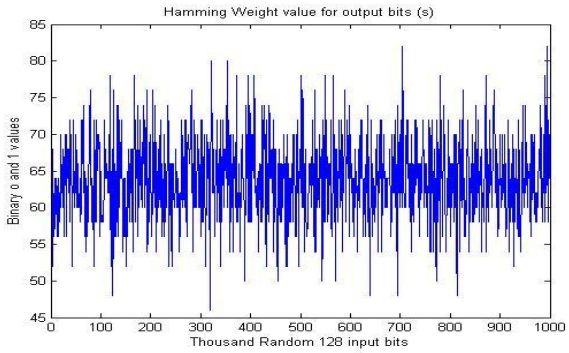

Fig 6. Hamming weight value

Fig 6 shows the hamming weight values for the thousand random generated inputs (x). The Hamming weight of a string is the number of symbols that are different from the zero-symbol of the alphabet used. It is thus equivalent to the Hamming distance from the all-zero string of the same length. It gives the average of 65 non zero values for 128 bit input. So for 128 bit input the calculated hamming weights gives almost 50% of the values of zeros and ones are evenly distributed.

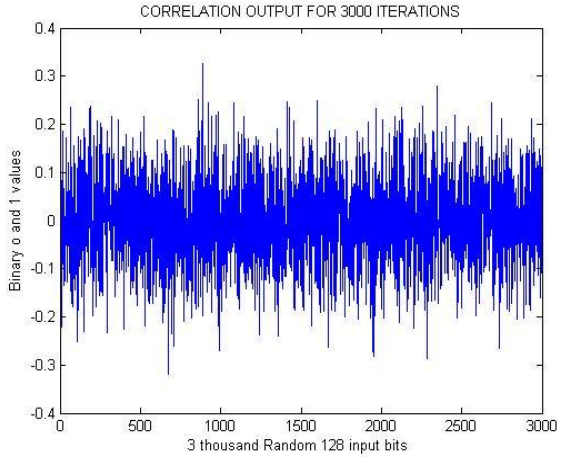

Fig 7. Correlation Output

From the fig 7 correlation function is a statistical correlation between random variables at two different points in space or time, usually as a function of the spatial or temporal distance between the points. For better correlation factor the value should be near to zero. From the graph for 3000 random inputs got the value almost closer to -0.2 to 0.2.

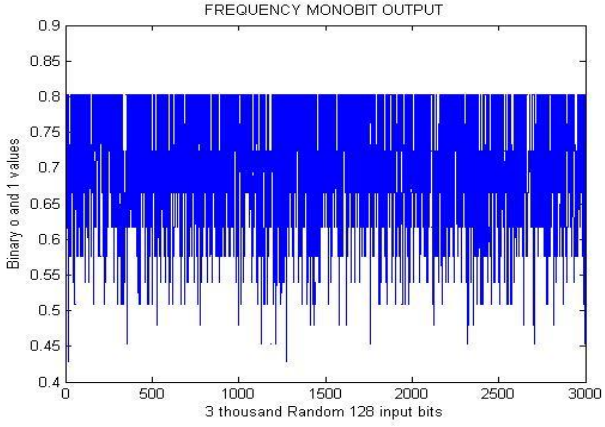

Fig 8. Frequency Monobit Test Output

From the frequency monobit test output graph the condition for the better randomness is the value should be greater than zero. Ihe frequency monobit is represented to test the random distribution of ones and zeros in the output sequence of the stream cipher. The keystream output of the cipher is truly randomness if the complementary error function value is > 0.01. In the fig. 8,

the error function P-value is found to be greater than 0.4 and the generated values are almost in the region of 0.8 for 3000 random data. Hence, the keystream of the stream cipher is highly random in nature.

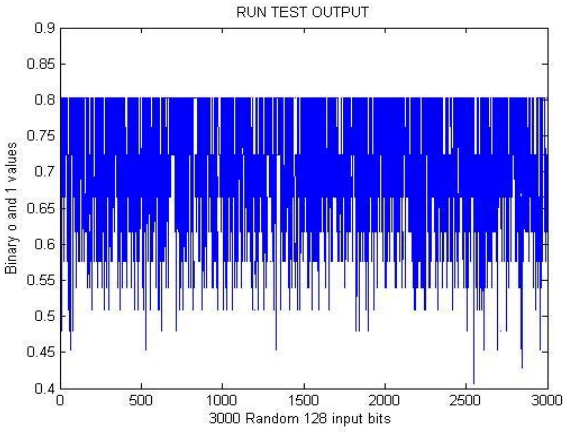

Fig 9. Runtest Output

Fig 9 run test output graph the condition for the better randomness is the value should be greater than zero. Ihe frequency monobit is represented to test the random distribution of ones and zeros in the output sequence of the stream cipher. The keystream output of the cipher is truly randomness if the complementary error function value is > 0.01. In the fig. 9, the error function P-value is found to be greater than 0.4 for 3000 random data. Hence, the keystream of the stream cipher is highly random in nature.

IV. CONCLUSION AND FUTURE WORK

In this paper, initially the various two dimensional (2D) cellular automata rules lik 15, 30, 45, based functions are chosen to test its non-linearity and balanced property by calculating mean and variance of hamming distance and hamming weight. The CA rule 15 and 30 seems to have best non-linearity and balanced property. The non-linearity and autocorrelation criteria are tested to these CA rule based von neumann functions. Von neumann Functionality has implemented with the designed cipher. The functionality verification tests like frequency monobit, and runtest has successfully done. So the designed algorithm has satisfied the necessary criteria and generates the better randomness.

In future, optimized and synthesizable VHDL code can be developed for the implementation of Von Neumann Functionality with the cellular automata concepts in the designed stream cipher. Each program can be tested with some of the sample vectors and output results are perfect with minimal delay. Therefore, designed stream cipher which can indeed be implemented with reasonable efficiency on an FPGA, and the performances are analyzed in terms of area, power consumption and throughput.

REFERENCES

[1] Bogdanov. A, Knudsen. L.R, Leander. G., Paar. C, Poschmann. A. Robshaw, M.J.B.,Seurin. Y, Vikkelsoe. C.: PRESENT: “An Ultra-Lightweight Block Cipher”, 2007.

[2] Dawei Li ; Inst. of VLSI Design, Zhejiang Univ., Hangzhou ; Yier Jin ; HaibinShen ; Xiaolang Yan “Design of Random Number Generation Algorithm” Publication Year: 2006 , Page(s): 1287 – 1290.

[3] Jegadish Kumar.K.J, .Chenna Kesava Reddy.K, Salivahanan.S.: “Novel and Efficient Cellular Automata based Symmetric Key Encryption Algorithm for Wireless Sensor Networks”. In: International Journal of Computer Applications (0975 – 8887) Volume 13– No.4, January 2011.

[4] Knudsen. L.R., Leander. G, Poschmann, A., Robshaw. M.J.B, PRINTCipher: “A Block Cipher for IC-Printing”. In: Mangard and Standaert [37], pp. 16–32, 2005

[5] Puczko. M. , Yarmolik. V.N “Designing cryptographic key generators with low power consumption “Year: 2006 .

[6] Wolfram. S, “Cryptography with Cellular Automata,” Crypto ’85, LNCS 218, Springer-Verlag, pp. 429- 432, 1986.

[7] Toffoli, Tommaso, and Margolus, Norman, “Cellular Automata Machines”, The MIT Press, Cambridge, Massachusettes, 1987.

[8] Zuohu Liu , Minghe Huang , Shaojun Zhu “The Design and Implementation of a Pseudo Random Number Generation Algorithm “Computational Intelligence and Natural Computing, 2009. CINC '09. International Conference on 2009, Page(s): 126 – 129.