IMPLEMENTATION OF OBJECT ORIENTED ENCRYPTION SYSTEM USING LAYERED CELLULAR AUTOMATA

CHINTA SOMSWARA RAO
Assistant Professor, Department of CSE, SRKR Engineering College, BHIMAVARAM, WEST GODAVARI, AP, INDIA.
chinta.someswararao@gmail.com

SRINIVASA RAO ATTADA
Assistant Professor, Department of CSE, Prajna Institute of Technology and Management, PALASA, SRIKAKULAM, AP, INDIA.

MADINA JAYANTHI RAO
Assistant Professor, Department of IT, SISTAM Engineering College, SRIKAKULAM, AP, INDIA

KUNA NAGESWARA RAO
Assistant Professor, Department of IT, SISTAM Engineering College, SRIKAKULAM, AP, INDIA

Abstract:
As the technology advances day by day, sharing of information through Internet is growing rapidly, which increases new information threats and vulnerabilities and hence the need to protect information to ensure its confidentiality, integrity, and authenticity require constant enhancements. Over the past two decades Cryptographic techniques are essential component of any secure digital communication. Cryptographic algorithms like DES, IDEA, AES etc., are proposed to provide high confidentiality, authenticity and integrity. With the rapid growth in the technologies, the processing speeds are increasing and as a result some of the algorithms are becoming obsolete and some require higher key lengths.

In this paper a strong time efficient cryptosystem is proposed. A novel approach in cellular automata is used in which the plain text is arranged into layers of binary digital planes and then encrypted based on the rule set of Automata. This scheme exhibits strength by inheriting the naïve properties of Cellular Automata, unpredictability, homogeneity, parallelism and sensitivity to the initial conditions. The proposed scheme is analyzed for time efficiency and observed to possess better confusion and diffusion properties when compared with Advanced Encryption Standard (AES). This scheme has advantage, that it has variable key size and block size; depending on the size of the plain text chosen. Simulation results show that the proposed system is on par with AES.

Keywords: Object Oriented Approach; Encryption; Decryption; cellular automata.

1. INTRODUCTION

Since the past decades to nowadays, cryptography is part of our everyday lives, being found in such commonplaces as gas meters, cash payment systems, vehicle alarms, maritime charts, TV signal scramblers, the internet, and so forth. The evolution of cryptography has been paralleled by the evolution of cryptanalysis — of the "breaking" of codes and ciphers. In 1917, the breaking of the Zimmerman telegram was instrumental in bringing the United States into World War I. The course World War II was dramatically altered by the cryptanalysts. The proliferation of computers and communications systems in the 1960s brought with it a demand from the private sector for means to protect information in digital form and to provide security services.
In 1970’s Feistel at IBM introduces the new secret key algorithm called DES (Data Encryption Standard) is the most well-known cryptographic mechanism in history. Later from 1975 to 1985 public-key algorithms like Diffie and Hellman, Rivest, Shamir, and Adleman known as RSA then after in 1991 Digital signatures are introduced.

1.1. Cryptography

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security.

In cryptographic terminology the actual/original information is known as plain text or clear text. Cipher text is the protected form of plain text and the process of converting plain text into cipher text using a cryptographic algorithm and a cryptographic key is known as Encryption and the process of converting cipher text into plain text using a cryptographic algorithm and a cryptographic key is known as the Decryption. When cipher text is correctly decrypted the result is recovered plain text. A mathematical function used to change plain text into cipher text (encryption) or vice versa (decryption). The function normally needs an extra parameter called the cryptographic key is called as Cryptographic Algorithm. A Cryptographic Key is a collection of one or more numerical parameters without which it is supposed to be hard for an entity to recover certain information which has been encrypted. Key also means the index under which parameters are stored in a database.

1.2. Cellular Automata

Cellular Automata is a discrete model that consists of grids of cells in which each cell can exist in finite number of states. Every cell can change its state based on the states of neighboring cells by following a prescribed rule. Cellular Automata with its inherent properties like Parallelism, Homogeneity, and Unpredictability, as well as it being easily implementable in both software and hardware systems, has become an important tool to develop cryptographic methods.

1.2.1. Physical view

1. A Cellular Automaton (CA) is an infinite, regular lattice of simple finite state machines that change their states synchronously, according to a local update rule that specifies the new state of each cell based on the old states of its neighbors.

2. Cellular automata are a collection of cells that each adapts one of a finite number of states. Single cells change in states by following a local rule that depends on the environment of the cell.

CAs are dynamical systems in which space and time are discrete, CAs exhibit some inherent features like parallelism, locality, simplicity, unpredictability and homogeneity thus cellular automata are naturally too fast, efficient in hardware and software implementations.

2. LITERATURE SURVEY

Cryptography has been a part of our everyday lives for some time now, here there is a need for more efficient and secure encryption algorithms; it makes sense to consider alternate techniques. Cellular automata as a medium for encryption are an attractive idea in theory because most CA can be implemented on very fast hardware hence a CA-based scheme may have the potential to encrypt and decrypt messages faster than existing techniques.

Most investigations into CA-based cryptosystems have been aimed at traditional secret key systems. There appear to be very few CA based public-key cryptosystems in the literature; one is the Finite Automata Public-Key Cryptosystem, although it uses non-homogeneous CA. Kar[1] outlines an idea for a public-key cryptosystem based on reversible cellular automata, and poses the question of how to implement the key generation algorithm. The objective of public-key cryptosystem based on reversible cellular automata (RCA) is to design an RCA that is very hard to invert without some secret knowledge. That way, the RCA can be published and its inverse can be kept as the private key.

A CA is said to be an RCA if for every current configuration of the CA there is exactly one past configuration (pre-image). If one thinks of a CA as a function mapping configurations to configurations, reversibility implies that this function is objective. For one dimensional CA there are known algorithms for deciding whether a rule is reversible or irreversible. For CA of two or more dimensions it has been proved that the reversibility is undesirable for arbitrary rules. For finite CAs that is not reversible, there exist patterns for which there are no previous states. These patterns are called Garden of Eden patterns. In other words, no pattern exists which will develop into a Garden of Eden pattern
2.1. Multi-layered Cellular Automata

Recently the concepts of Multi-layered Cellular Automata (MCA) are studied by RaminAyanzadeh et al [2]. The concept of multi-layer cellular automata (Figure 1) and a novel neighborhood structure is introduced from that a new approach for generating normal random numbers is proposed. First layer consists of binary cellular automata which are responsible for activating and inactivating cells in next layers. A cellular automaton with integer values is used for these layers. Interaction between layers of represented cellular automata leads to a dynamic and complex behavior of proposed model. Multi-layer cellular automata generate better normal random numbers.

![Multi-layered CA for generating normal pseudo random numbers](image)

Fig. 1. Multi-layered CA for generating normal pseudo random numbers

2.2. PRNS generation using Cellular programming

The PRNS generation depends upon the rules applied on the cellular automata, if good rules are applied good quality of PRNS is generated, to identify good rules from the set of available rules for that here an evolutionary approach called cellular programming, in that the behavior of each rule is studied and the PRNSs generated by that rule is tested, if the rule performance is good and it passed all the NIST standard then those rules are taken applied on the CA to generate the PRNS, this PRNS acts as secret key in encryption process.

Cellular Programming is an evolutionary computation technique introduced to discover rules for non-uniform CAs. Figure 2 shows a CP system implemented to discover rules. The system consists of a population of N rules and each rule is assigned to a single cell of CAs. After initiating states of each cell, i.e. setting an initial configuration, the CAs start to evolve according to assigned rules during a predefined number of time steps. Each cell produces a stream of bits –PRNS. After stopping evolving CAs all PRNSs are evaluated. The entropy $E_h$ is used to evaluate the statistical quality of each PRNS. To calculate a value of the entropy each PRNS is divided into subsequences of a size $h$. In all experiments the value $h = 4$ was used. Let $k$ be the number of values which can take each element of a sequence (in our case of binary values of all elements $k = 2$) and $k^h$ a number of possible states of each sequence ($k^h = 16$). $E_h$ can be calculated in the following way:

$$E_h = - \sum_{j=1}^{k^h} p_{h_j} \log_2 p_{h_j}$$

Where $p_{h_j}$ is a measured probability of occurrence of a sequence $h_j$ in a PRNS. The entropy achieves its maximal value $E_h = h$ when the probabilities of the $k^h$ possible sequences of the length $h$ are equal to $\frac{1}{k^h}$.

It is worth to mention that the entropy is only one of possible statistical measures of PRNSs. It will be used as a fitness function of CP. To decide about final statistical quality of PRNSs and a suitability of discovered rules for cryptography purposes some additional tests must be conducted [3].
2.3. Secret key Generation using CA

Franciszek Seredyński et al. [4] described the process of generating the PRNS, which makes the strong encryption keys. During the generation of PRNSs they have been taken one dimensional (1D), non-uniform CA. The quality of PRNSs highly depends on a set of applied CA rules; those rules are identified using CP. As the result of collective behavior of discovered set of CA rules very high quality PRNSs are generated. The quality of PRNSs outperforms the quality of known one dimensional CA-based PRNS generators used in the secret key cryptography. The extended set of CA rules which was found makes the cryptography system much more resistant on breaking a cryptography key. The same process is reviewed by Tomassini & Sipper [5] instead of using 1D they considered 2D, various neighborhood structures are used, by this process also the generated PRNSs are very strong and resistant against cryptographic attacks, later this has been extended to multi-dimensional cellular automata.

2.4. Block Encryption using CA

2.4.1. Block encryption using Elementary CA

Petre Anghelescu et al. [6] presented an encryption system implemented on a structure of Hybrid Additive Cellular Automata (HACA) used for securing data sent over the internet. They used the combination of Hybrid CA and Additive CA. Along with that they used the chaotic rules for providing good security. Samir Kumar Bandyopadhyay et al. [7] used CA in DES and AES.

2.4.2. Block encryption using RCA

XIA Xuewen et al. [8], traditional reversible cellular automata (RCA) is fit for cryptography for its rules being an affine function, i.e. one reversible CA’s rule can be applied in encryption process while another counterpart rule can be applied in decryption process. In order to improve the complexity of CA’s dynamics, which is a crux in cryptography, traditional CA model is replaced by multi-granularity cellular automata (MGCA). Based on MGCA and RCA a cryptography algorithm that is proposed which called MGRCA. In MGRCA, cells have different granularity and can adjust their granularity dynamically by “split-recombination” behavior during the process of encryption and decryption. A multi-granularity cellular automata (MGCA) is presented aimed to improve the dynamic complexity of CA. In MGCA, each and every iteration consists of two steps; one is state-change and other is split-recombination. The former step is similar to the iteration of traditional CA and the latter step demonstrates the split of bulky-granularity CA and the recombination of fine-granularity CA. It is undesirable if a given two-dimensional CA is reversible. This is true even when restricted to CA using the von Neumann neighborhood.

3. SYSTEM ARCHITECTURE

In the year 2009 XIA Xuewen et al. [8] has proposed data encryption using multi-granularity reversible cellular automata, in that only non-uniform cellular automata is considered. Later in the year 2010 Ramin Ayanzadeh et al. [2] has proposed multi-layer cellular automata and a novel neighborhood structure. According to these concepts, a scheme for generating normal random numbers is proposed. First layer consists of binary cellular automata which are responsible for activating and inactivating cells in next layers. A cellular automaton with
integer values is used for these layers. Interaction between layers of represented cellular automata leads to a dynamic and complex behavior of proposed model. Main idea of this model is based on central limit theorem to generate normal random numbers.

Proposed system deals with the Layered Cellular Automata (LCA) is considered, where in automata can be viewed as a system, that consists of layers, and each layer is consists of rows of 1D cellular automata. The proposed system named as Layered Reversible Cellular Automata (LRCA), which is the combination of LCA and RCA. LRCA is a block encryption technique (large block size) with symmetric key. The text is converted into binary form and arranged in layers later it is iterated to construct the cipher text. This arrangement of cipher text gives the good confusion and diffusion to augment the security.

In the proposed system a Layered Cellular Automata is considered where in the automata can be viewed as a system that consists of layers. The text is converted into binary form and arranged in layers (Figure 3) where each row is considered as a 1D CA with periodic boundary with radius equal to unity. 1D rule are used for encryption on each layer.

This system mainly divided into three modules as per the functionality. Figure 4 gives the diagrammatic representation of LRCA, which mainly contains the three modules as follows:

1. Rule set Generation
2. Encryption Process
3. Decryption Process

3.1. Rule set generation Procedure

Take some set of rules which are reversible, both the sender and receiver shall agree on those rules that are to be used along with indexes created for the rules for the particular encryption. They shall also agree on the index and size in the key to be used to generate the number of iterations along with shift indicators. A random series of indexes is generated to identify the particular rule that is to be used on each cell of a layer. A shift on the sequence of rules is applied from row to row by treating the rows on the all the layers sequentially.

**STEP 1. Select the reversible rules**

In this system 3-neighborhood structure is used, while this structure is considered there exist \(2^3 = 256\) rules. From those rules there are only 6 reversible rules. By taking the key size into consideration, the following sets of reversible rules are used. In each pair, first rule used for encryption and second rules used for decryption.

**STEP 2. Index the rules for both encryption and decryption**

Index the rules from zero, and then separate the encryption and decryption rules separately.

**STEP 3. Generate Random series**

Generate a series of random numbers consists of only index numbers (i.e. 0 to 3)

**STEP 4. Generate encryption and decryption Rule set**

Map the encryption rules to the above random numbers then collect that mapped series as encryption Rule set. To generate the decryption Rule set map the decryption rules to the random series.

**STEP 5. Shifting both encryption and decryption Rule set**

Shifting of Rule set can be done when moving from one layer to another layer which gives the good confusion and diffusion and also gives the unpredictability to an attacker.
3.2. Encryption Procedure

Divide the plain text into blocks of size 4096 characters (ASCII values for each character is considered so that there in total 4096*8 bits), (padding bits are added whenever needed) and the text is converted into binary sequence and the bits are arranged into 8 layers where each layer consists of 64*64 bits. Arrange the first bits of all the characters in the first layer and second bits of all characters in the second layer and continuing this process arrange the eight bit of all the characters in the eighth layer. Then apply a CA rule set on each cell of each layer and iterate each layer up to some predefined number of iterations, then each layer produce the cipher bits from each cell. Again the cipher bits are converted into text by converting them into ASCII values to produce the cipher text.

**STEP 1. Divide the plain text into blocks**

Take the data in the plain text and divide into blocks of size 4096 bytes, take each block perform the following steps.

**STEP 2. Take each block of plain text then repeat the steps from 3 to 5**

**STEP 3. Take each character’s binary sequence arrange that into layers**

Take the binary sequence of each character in a block then place first bit of all characters binary sequence in the first layer, second bit of all characters in the binary sequence in the second layer, like that last bit (8th bit) of all characters in last layer.

**STEP 4. Apply the encryption rule set on LRCA**

Apply the encryption rule set on each layer to move the layered reversible CA to its next state depends upon the number of iterations. The number of iterations is calculated based on the selection of index values; convert the each selected index values into binary combine the binary sequence of those index values to get the actual number of iterations.

**STEP 5. Gather all layers in LRCA to form the cipher text**

Take first binary bit in all the layers to form the binary sequence convert that into ASCII which gives the first character in cipher text, Take second binary bit in all the layers to form the binary sequence convert that into ASCII which gives the second character in cipher text, like that Take last binary bit in all the layers to form the binary sequence convert that into ASCII which gives the last character in cipher text.

3.3. Decryption Procedure

The cipher text is converted back to binary form and the sequence of rules used in encryption is generated from the key the corresponding reversible rules are used in the same manner that of encryption on each cell for a predefined number of iterations, and the corresponding plain text is extracted from the binary sequence.

**STEP 1. Divide the cipher text into blocks**

Take the data in the cipher text and divide into blocks of size 4096 bytes, take each block perform the following steps.

**STEP 2. Take each block of cipher text then repeat the steps from 3 to 5**
**STEP 3. Take each character’s binary sequence arrange that into layers**

Take the binary sequence of each character in a block then place first bit of all characters binary sequence in the first layer, second bit of all characters in the binary sequence in the second layer, like that last bit (8th bit) of all characters in last layer

**STEP 4. Apply the decryption rule set on LRCA**

Apply the decryption rule set on each layer to move the layered reversible CA to its next state depends upon the number of iterations. The number of iterations is calculated based on the selection of index values; convert the each selected index values into binary combine the binary sequence of those index values to get the actual number of iterations as shown in Figure 4.

**STEP 5. Gather all layers in LRCA to form the decipher text**

Take first binary bit in all the layers to form the binary sequence convert that into ASCII which gives the first character in decipher text, Take second binary bit in all the layers to form the binary sequence convert that into ASCII which gives the second character in decipher text, like that Take last binary bit in all the layers to form the binary sequence convert that into ASCII which gives the last character in decipher text.

### 4. RESULTS

**4.1. Brute Force Attack**

Brute force attack or exhaustive key search is a strategy that can in theory be used against any encrypted data by an attacker who is unable to take advantage of any weakness in an encryption system that would otherwise make his/her task easier. It involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space.

The key length used in the encryption determines the practical feasibility of performing a brute force attack, with longer keys exponentially more difficult to crack than shorter ones. Brute force attacks can be made less effective by obfuscating the data to be encoded, something that makes it more difficult for an attacker to recognize when he/she has cracked the code. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute force attack against it.

**4.2. Confusion**

Confusion refers to making the relationship between the key and cipher text as complex as possible and it is observed that the number of bits changed in the key results the number of bits changed in cipher text.

**4.2.1. Comparison of confusion property with AES**

Figure 5 gives the confusion levels of proposed algorithm are compared with AES algorithm by taking plain text of size 4k with key size 128 bit. It is observed that confusion levels obtained by the proposed algorithm are almost same as that of AES with marginal betterment.
4.2.2. Confusion property of LRCA with different keys

Figure 6 gives the confusion property of proposed algorithm, which is tested with various keys applied on same plain text gives nearly 50% to 55% change in cipher text.

![Fig. 6 Confusion property of LRCA different keys and same plain text](image)

4.3. Diffusion

Diffusion refers to making the relationship between the plain text and cipher text as complex as possible and it is observed as the number of bits changed in the plain text results the number of bits changed in cipher text.

4.3.1. Comparison of diffusion property with AES

Figure 7 gives the diffusion levels of proposed algorithm are compared with AES algorithm by taking plain text of size 55bytes with key size 128 bit. It is observed that diffusion levels obtained by the proposed algorithm are better as compared with AES.

![Fig. 7 Diffusion property of LRCA and AES](image)

4.3.2. Diffusion property of LRCA with different plain texts

Figure 8 gives the diffusion property of proposed algorithm, which is tested with same key applied on various plain texts gives nearly 75 to 80% change in cipher text.
4.4. Time analysis of LRCA and AES

The encryption and decryption processes are taken together and it is observed that the time taken by LRCA is less than AES when same plain text and key used in both algorithms varying the size of the plain text. Figure 9 and Table 1 gives the comparison of proposed algorithm and AES with respect to time.

![Figure 8: Diffusion property of LRCA with same key and different plain text](image)

![Figure 9: Comparison of LRCA and AES with respect to time](image)

**Table 1. Timing analysis between LRCA and AES**

<table>
<thead>
<tr>
<th>S. No</th>
<th>Plain text (KB)</th>
<th>LRCA (ms)</th>
<th>AES (ms)</th>
<th>Reduction (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>402</td>
<td>406</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>416</td>
<td>422</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>447</td>
<td>454</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>578</td>
<td>582</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>24</td>
<td>601</td>
<td>608</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>32</td>
<td>766</td>
<td>772</td>
<td>6</td>
</tr>
</tbody>
</table>

5. CONCLUSION AND FUTURE WORK

As proposed in this thesis a layered cellular automata has been successfully implemented to improve security data encryption in terms of confidentiality, authenticity and integrity, this system is tested and proven that the
system performs better than the existing system AES. As this layered approach in cellular automata uses the interesting features of CA like parallelism, simplicity, locality and unpredictability gives enough strength to the encryption system. In this system the possibility of arranging text into layers of Cellular Automata, which results a new novel neighborhood system, based on which a secure encryption method is developed. The proposed method is compared with AES for various parameters like confusion, diffusion and time gives the better results.

The proposed system is developed and analysis is done along with AES on various sizes of plain text and results are evaluated. AES shows that proposed system exhibits good confusion and diffusion properties and is time efficient than AES.

**Future Work**

Each cell except the boundary cells is having 8 neighbors in its plane and the cells that lie on the planes other than the top and bottom are having 26 neighbors. This approach in principle invokes possibility of defining transformation functions based on the neighbors of different layers and can be of order of $2^{58}$. This may lead to analysis of a new class of CA and is much of theoretical interest.

**References**


