Cryptanalyze shift register based-Stream Cipher Using Innovative DNA Trees Clustering Model to

Basim Sahar Yaseen

Department of Computer Sciences-Shatt Al-arab University College
Email: basimsahar@sa-uc.edu.iq

https://doi.org/10.31972/iceit2024.014

Abstract

The paper presents a novel approach that merges the abilities of the biological environment with the concept of hierarchical trees to attack a specific stream cipher. The model being presented introduces a systematic method that targets a group of stream ciphers, such as the GCM family, these devices are composed of components that are suitable for the proposed method. A restricted set of binaries for the final key sequence is required to implement this technique as an input. The attacked algorithm comprises feedback shift registers, memories, delays, and so on. The stream ciphers are widely used in modern encryption to secure communication devices, so any attempt to analyze or attack it is of the utmost importance. The results of this method have been confirmed to lead to the destruction of the cipher's security. Many novelties and contributions of the present work can be summarized as follows: firstly, the key generator's components are attacked individually, disrupting the cohesion between them. This was not possible previously except in rare cases and under difficult conditions. Secondly, the method of verifying the correct initial values is unrelated to the generator's operation. Thirdly, the technique applies biological concepts and processes to laboratory test tubes for genetic engineering, it can be said that the prepared model targets a broad class of stream key generators, rather than a single algorithm. The proposed technique requires a specific and deterministic number of final key sequence bits, which are easy to provide. The proposed technique creates a search Ɛ-tree in the style of hierarchical clusters, in which the first level contains Ɛ nodes. Then each successive level contains the square of Ɛ nodes of the number of nodes in the previous level, and the root is composed of the total solution space of the stream key generator and produces the nodes of each level from the intersection of the cluster contents in the test tubes for all clusters in the level above it. The contribution and novelty of the present work is cryptanalyzing and attacking shift register-based stream key generators involves fragmentation. The attacking principle entails disassembling generator components from registers and individually attacking them. DNA logic clustering aids in this process, as the strength of these generators relies on component cohesion. Because the components are cryptanalyzed individually, the time complexity of the attack is equal to $O(C2^N)$, where N is the length of the largest component, and C is a constant.

Keywords: shift register, DNA-Based Cryptanalysis, Stream Cipher, Attacking, Hierarchal Trees.

1 Literature Review

It is possible to use the capabilities of the biological environment to improve cryptanalysis, which is called relative exploitation. The success of this method depends on how much of these capabilities are utilized. There are two main approaches to this kind of work. The first involves using genetic base encodings to generate information and then applying traditional cryptanalysis algorithms. This method is the most common. The second approach is the real approach to using the potentials of the biological environment in the field of attacking and cryptanalysis is a DNA-based cryptanalysis, which employs DNA computing models and operations. This method is less common than the first. There have been successful cases of using the second approach in DNA-based cryptanalysis of stream cipher in recent years, although it is rare. One of the most prominent works in this field: A recent paper introduced an algorithm for cryptanalysis of an encrypting image using a 2D Hénon-Sine map and DNA coding approach. However, it has been discovered that the algorithm is not as secure as originally claimed. The encryption scheme employs a permutation-diffusion architecture with DNA random coding and exclusive OR for image diffusion. Additionally, pixel-swapping operations are used for image scrambling. [1]. The following text describes a new method for encrypting images using a Feistel network and dynamic DNA encoding. It involves four steps to encrypt plain images, including generating chaotic sequences, Hill encryption, Feistel network, and Pixel diffusion. However, the paper highlights some issues with the secret key design and encryption process of this encryption scheme and proposes necessary improvements to address them. Additionally, the paper introduces a corresponding chosen plaintext attack algorithm [2]. The paper explains how the logic of keystream bits is transformed from propositional logic to DNA logic and executed in polynomial time. It treats each binary component of the final key chain as a collection of logical components, and its default values can be guessed, thus reducing the possibility of incorrect values. This guess continues along the series of binaries being processed, so this method becomes more complex as the number of binaries processed increases [3]. The following paper suggests a sticker DNA model to cryptanalyze the cipher created by the keystream of linear and nonlinear feedback shift registers. The model is based on the principle of establishing a binary sequence as a memory strand that represents the potential plain text sequence. Subsequently, it creates all possible paths to find the correct solution by linking the stickers to the components of the solution paths that represent the key parts [4]. The study suggests a method that utilizes the GA and DNA sticker model to perform a parallel search and attack on a cryptosystem. The technique involves creating a database of all possible solution paths in the first step. The proposed combination of algorithms is then used to search for the correct path. [5]. A proposed modified digital simulation of the DNA sticker model technique combined with another technique to attack linear and nonlinear feedback shift register generators, the sticker model can serve efficiently parallel search with constructing data base for all searching paths [6]. The paper introduces a new method called the DNA sticker model for cryptanalysis of a stream cipher that uses a key stream sequence generated from a linear shift register. The cipher sequence is decrypted by applying sticker operations at the binary level. Despite the positive aspects of this work achieved within DNA-based cryptanalysis, it

suffers from dealing with the components of the final sequence as a single block, and therefore it searches for the initial values of the shift registers as a single component and with a complicated complexity for all the shift registers. [7]. It suggests the creation of a software computer that uses genetic operations based on a splicing DNA model. It also uses a probabilistic model of the English letter frequency in a vertical alignment. This software aims to generate genetic bases of the strands, which represent the letters of a natural language. The cohesion of these bases may depend on the frequency of occurrence of these letters in the plain text or key [8]. A DNA splicing model is introduced that can cryptanalyze a stream cipher sequence generated by an unknown source. However, the cipher is known to be encoding for the plaintext. The proposed model utilizes the statistical properties of the plaintext along with the random properties of the key string segments, The paper harnesses the processes of cutting and ligating DNA sequences based on the verification of plain text specifications in the community of generated sequences, and this method does not always give certain results. [9]. All of these works achieved results within the targeted LFSR-based stream cipher, whether the results were complete or partial. Still, the targeting was for a specific and deterministic encryption algorithm and not any other. Table 1, It is a comparison between works that achieve the concepts of DNA-based cryptanalysis, whether the proposed technique or other works mentioned, which attacking the LFSR-based stream cipher. The proposed model is unique in its method of individually attacking the components of stream key generators, which is reflected in the time and complexity of the attack.

Table 1: A Comparison between the proposed model with the other techniques.

Reference	The Method	Cryptanalysis Type	Approach of Attack or Cryptanalysis	Evaluated Complexity
[3]	DNA logic technique	conventional cryptanalysis technique to cryptanalysis DNA coding	Key Stream (Z_i)	It depends on how long Z_i is processed
[4]	Sticker DNA model	DNA-Based Cryptanalysis	Combined FSRs	Adopting a parallel search
[5]	GA with Sticker DNA	DNA-Based Cryptanalysis	Combined FSRs	Adopting a parallel search
[6]	Sticker DNA model	DNA-Based Cryptanalysis	Combined FSRs	=
[7]	Sticker DNA model	DNA-Based Cryptanalysis	Combined FSRs	=
[8]	Splicing DNA model	DNA-Based Cryptanalysis	Combined FSRs	=
[9]	Splicing DNA model	DNA-Based Cryptanalysis	Combined FSRs	=
Proposed model	Clustering by using Test Tube operations	DNA-Based Cryptanalysis	FSRs Individually	Adopting a parallel search and partitioning the generator.

2 Introduction

The concept of clustering is the process of organizing a set of objective features into groupings named "clusters". Features inside a cluster are highly similar in shape, function, yields,..so on, whereas the clusters are as diverse as possible. Clustering's purpose is to generalize, classify, and expose a relationship between object attributes. Clustering tools automatically group points or areas into compact clusters, while placing optional constraints on the clusters such as minimum and maximum size, or a balanced total field, such as distributed populations. In cryptology applications, such as cryptanalysis, grouping may take the meaning of isolating initial values and classifying them according to their fulfillment of the values resulting from the digital sequences of partial or final outputs, or grouping may be according to the effect of those values on the work of the cipher generator parts. DNA sequence clustering has broad applications in molecular biology. Clustering tools have been applied to the clustering of transposable elements, open reading frames, and expressed sequence tags. Cluster analysis has been used as a “supplement” to evolutionary analysis. Clustering tools have been used to identify subtypes in a viral population, identify “representative non-reference sequences” needed for genome construction, decompose genomes, and “assign individuals” to operational taxonomic units. Using DNA barcodes [10].

To date, there is no molecule more suitable for IT applications [11] than DNA [12]. Nucleic acids possess the fundamental property of the Watson-Crick [13] rule, Figure 1, depicts the principles of the new rule, which is the basis for many DNA manipulation techniques, allowing for a unique range of potential applications for computational purposes across disciplines. These processing techniques were built on the biologically sophisticated properties of the DNA molecule and were originally developed for the life sciences but have since been gradually reused in computer applications. Late in the last century, this technology came into use to solve difficult cryptographic problems. It can be solved by traditional methods [14]. The idea behind DNA-based cryptanalysis [15,16] is to use biomolecular components, the processes performed on them in the laboratory, the biocomputational models derived from them, and the test tube processes performed on them in the laboratory to accomplish complex and difficult computing tasks, instead of electronic and silicon components that were unable to accomplish them. These are the tasks that we use in traditional computing. Although the computational models proposed and the processes exploited by DNA computing [17] vary, there are fundamental processes that have been used in test tubes in the biological laboratory and are used in every biocomputational technique invented to solve a problem, and these processes are annealing, Ligase, melting, is-empty, is-full, ... Figure 2 shows the processes of annealing and ligase that take place in the laboratory and that can be performed on the digital representation of the genetic bases. The use of unconventional techniques [18] in cryptanalysis and attacking cryptographic systems [19], such as biological technology because of its well-known capabilities, opens horizons for discovering fatal weaknesses in these systems, in addition to overcoming the difficulties of attacking them. When evaluating and analyzing encryption techniques and algorithms, cryptanalysis is a fundamental scientific field on which cybersecurity [20] depends. In the past few decades, forensic science has been enhanced by adding DNA technology, which has brought powerful capabilities.

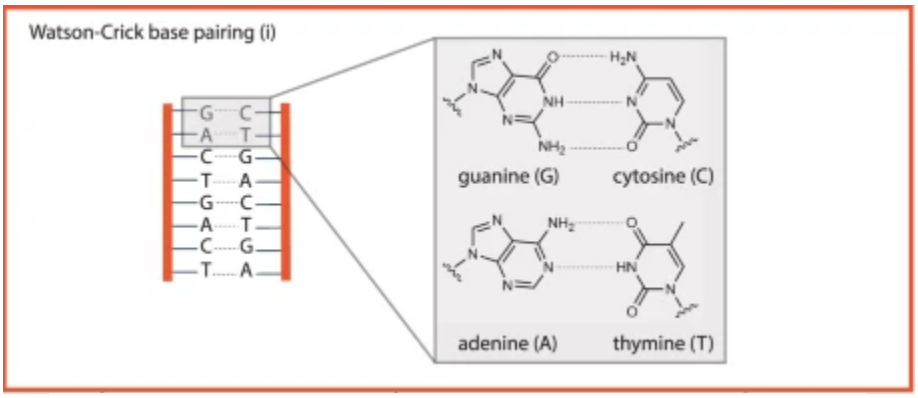


Figure 1: the principles of the Watson-Crick rule of the genetics [12].

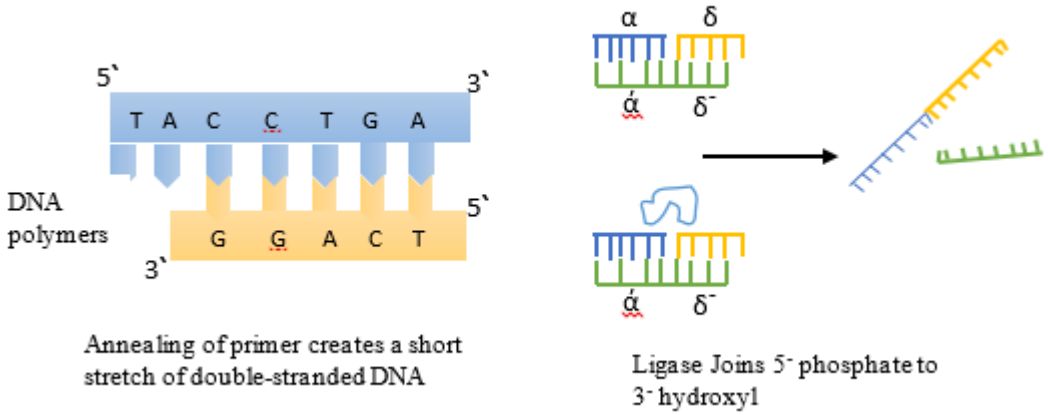


Figure 2: Annealing and Ligating operations by polymers [12].

3 The Proposed Model

The proposed cryptanalysis method is a known plaintext attack, so there must be knowledge of a specific number of plaintext bits (the required bits number ≈ 10 bits and more), which are substituted in the equation for calculating the ciphertext, Eq. (1), and extracting a specific sequence of the final keystream bits Z_i .

$$Z_i = C_i \text{ XOR } P_i \quad \text{, where } i=1,2,..,128 \qquad (1)$$

Like most LFSR-based stream key generation algorithms, the final XOR function can be considered a logical function that combines the outputs of the four LFSRs(if no. of components is 2)to give the summed result as part of the final key sequence Z_i, Eq.(2).

$$RS_i = LFSR_{1i}\text{-out XOR } LFSR_{2i}\text{-out} \qquad (2)$$

Where RS_i is the binary value summation at the location i of the Z_i sequence, and $LFSR_{ji}$-out is the output of the linear shift register j at i location of the Z_i.

Depending on the binary value, the output can be treated as one of the following logical values, which are described according to the propositional logic, Eq.(3), all logical value probabilities of the Z_i bits :

$$S_i = R_{1i}R_{2i} \text{ OR } \overline{R_{1i}}\overline{R_{2i}} \text{ OR } R_{1i}\overline{R_{2i}} \text{ OR } \overline{R_{3i}}\overline{R_{4i}} \qquad (3)$$

Where R_{ji} is the output of the $LFSR_j$ at location i in the Z_i sequence, R_{ji} is the complement bit of R_{ji}. The logical function between LFSRs in this formula is XOR.

So, true structures above, Eq. (3) can be considered as measures for tube sets, Eq. (4):

$$RS_i = M1 \text{ OR } M2 \text{ OR } M3 \text{ OR } M4 \text{ , where } M1 = R_{1i}R_{2i} \text{ and } M4 = \overline{R_{1i}}\overline{R_{2i}} \qquad (4)$$

The hierarchical DNA clustering model is recursively clustering DNA points into many clusters at each level. A genetic keystream can be represented by a Ɛ-degree tree, depending on the number of genetic bases of the first level of clusters(nodes) as in Table 1. As shown in Figure 3-a, many encryption systems and algorithms rely on the shift register's physical component and the avalanche concept to ensure their security. This makes it difficult for attackers to dismantle the components of the shift registers and attack them individually. Experts and stakeholders consider these components' increasing complexity and large size as a strength factor for these systems.

3.1 The Methodology

Based on equations number 3 and 4, the basic number of test tubes is 4. The proposed digital model is based on a model that was used in a biological laboratory where each cluster represented as test tube. The model generates a set of test tubes containing the remaining basic strands that result from various reactions. The following are the main steps involved in the process:

1) Initialize genetic base strands for all initial values for the generator components.
2) Separate the strands' groups that verify the genetic bases of the keystream into individual test tubes.
3) Transect each level of the strand's groups consecutively, starting from the first level.
4) Extract the repetitive strands from all of the test tubes belonging to the groups of first-level strands.
5) Check all the test tubes belonging to the groups of first-level strands if:
   a) If is empty then exclude it.
   b) If is not empty then be a candidate as a potential solution.

However, a proposed digital model challenges the cohesion of these systems through the principle of fragmentation by attack. It works by fragmenting and attacking the shift registers and then reducing the initial values that they adopt to produce the final key sequence. The principle of reduction depends on the concept of clustering, which involves creating clusters of solutions space whose contents are interrupted and reduced at each level of the Ɛ-degree tree that is created for the genetic bases of the key sequence, taking into account that A's complement is T (00 -> 11). C's complement is G (01 -> 10). The model involves two specific processes - a

divide-and-conquer approach and a DNA Ɛ-degree tree clustering process - which significantly reduces the solution space and searches for the initials of components such as LFSRs and NLFSRs. This approach differs from known attack methods that target registers together and surpasses the avalanche characteristic of the stream cipher. A specific set of keystream binaries must be obtain[illegible]ent methods to obtain these binaries, such as guessing or predicting the letters of the plaintext. The number of bases needed is proportional codes to the number of keystream components required to transform the key stream into a series of genetic bases. These bases are essential to produce a genetic base sequence from the key stream outputs. Table 2 determines the genetic bases, value of Ɛ, and codes for 2,3,4 device's components are required to proportional codes to the number of keystream components.

Table 2: The genetic bases and codes of the Ɛ-degree tree

No. of components	**No. of Codes**	**Ɛ-degree Tree**	**Codes of the Clusters**
2	4	4	A, T, C, G
3	8	8	0A, 0T, 0C, 0G, 1A, 1T, 1C, 1G
4	16	8	AA, AT, AC, AG, TT, TA, TC, TG, CC, CA, CT, CG, GG, GA, GT, GC

To accurately describe the operation of the model, we consider the target system as consisting of multiple linear feedback shift registers. The outputs of these registers are then summed up using a linear function such as XOR, as shown in Figure 3-b.

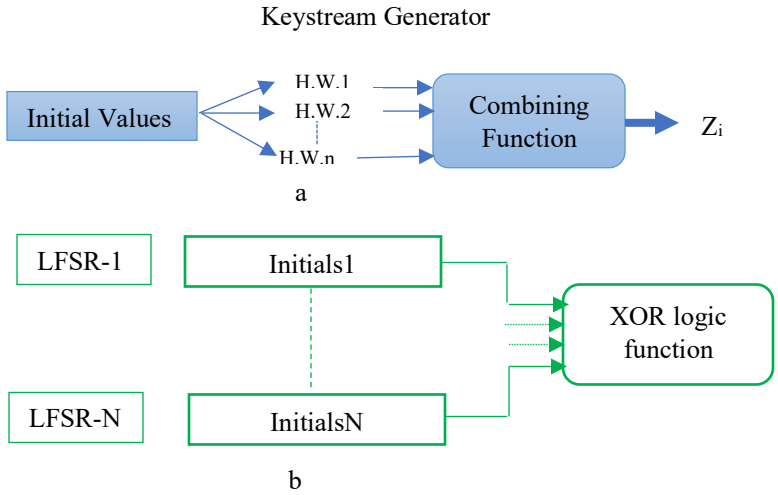


Figure 3: Architectures of targeted SC generators, a- overall SC architecture.
b- The architecture of the generator attacked by the model.

Based on the given system, the hierarchical search tree takes Figure 4.

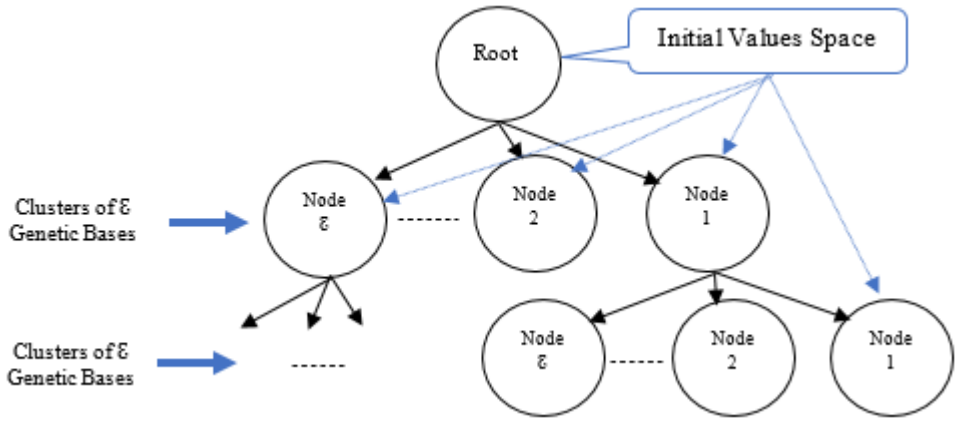


Figure 4: The shape of the hierarchical search tree of Ɛ-degree

We are constructing the Model by using Test Tube (TT) operations. $TT_{Universal}$ "The test tube that contains all the initial values for all LFSRs, $Z_{GB(i,j)k}$ is the final bit k of the key sequence, with codon genetic bases i and j.

Let:

- FSR_1, FSR_2,…, and FSR_n is a feedback shift that registers components of the stream key generator.
- Z_i is a final key sequence. $Z_i = FSR_{1i}$ xor FSR_{2i} ,…, xor FSR_{nj} ,where i=1,…,j.
- Ɛ is the degree of the tree (number of node connections).
- No. of required level is L.
- The Z_i sequence that is produced,
  $Z_{GB\ (1,2,\ldots)1}$, $Z_{GB(1,2,\ldots)2}$, $Z_{GB(1,2,\ldots)3}$, $Z_{GB(1,2,\ldots)4}$, $Z_{GB(1,2,\ldots)5}$, …. ,$Z_{GB\ (1,2,\ldots)L}$.
  When Z_i =0 →Z_i is $Z_{GB\ (A,\ T,\ldots)i}$ or $Z_{GB(C,G,\ldots)i}$ or …
  Z_i =1 →Z_i is $Z_{GB\ (C,\ T,\ldots)i}$ or $Z_{GB(G,A,\ldots)i}$ or …

Algorithm Building and searching within a Hierarchical DNA Ɛ-degree Tree.
Input: Solution Spaces values of FSR1, FSR2, …. Genetic Bases of Keystream ($Z_{GB(\_,\_)i}$).
Output: Correct FSR initial values.
Steps:
(*Searching by Divide-and Conquer phase *)
For all Solution Space Values of FSR_1
For i:1 → L

IF initial=$Z_{GB(1,\_)i}$ → initial → $TT_{CLUSTER1i}$
IF initial=$Z_{GB(\_,2)i}$ → initial → $TT_{CLUSTER2i}$
Loop
Loop
For all Solution Space Values of FSR_2
For i:1 → L
IF initial=$Z_{GB(1,\_)i}$ → initial → $TT_{cluster1i}$
IF initial=$Z_{GB(\_,2)i}$ → initial → $TT_{cluster2i}$
Loop
Loop
For all Solution Space Values of FSR_j
For i:1 → L
IF initial=$Z_{GB(j,\_)i}$ → initial → $TT_{cluster1i}$
IF initial=$Z_{GB(\_,j+1)i}$ → initial → $TT_{cluster2i}$
Loop
Loop
(***Phase of Building the Ɛ-degree Tree and Searching within it** *)
So, $TT_{clusterj+1i}$ is the $\overline{TT}_{clusterji}$ (inverse)
$TT_{universal} = TT_{FSR1}. \cup TT_{FSR2,\ldots,} TT_{FSRn}.$
$TT_{universal} = TT_{cluster11} + TT_{cluster21},+\ldots+ TT_{clusterji}$ ($TT_{universal}$ the root of the binary tree)
For i:1 → L
For j:1 → no.of FSR initials
$TT_{cluster1i+1} = TT_{cluster1i-1} \cap TT_{cluster1i}$ (all initials j that satisfy GB1i)
$TT_{cluster2i+1} = TT_{cluster2i-1} \cap TT_{cluster2i}$ (all initials j that satisfy GB2i)
$TT_{clusterji+1} = TT_{clusterji-1} \cap TT_{clusterji}$ (all initials j that satisfy GBji)
Loop
For j:1→ 2^i
IF $TT_{cluster1i+1}$ is-empty → remove $TT_{cluster1i+1}$
IF $TT_{cluster2i+1}$ is-empty → remove $TT_{cluster2i+1}$
IF $TT_{clusterji+1}$ is-empty → remove $TT_{clusterji+1}$
Loop
Loop
For j:1→ 2^i
IF $TT_{cluster1i+1}$ not is-empty → $TT_{cluster1i+1}$ is a solution.
IF $TT_{cluster2i+1}$ not is-empty → $TT_{cluster2i+1}$ is a solution.
IF $TT_{clusterji+1}$ not is-empty → remove $TT_{clusterji+1}$
Loop
End of the algorithm

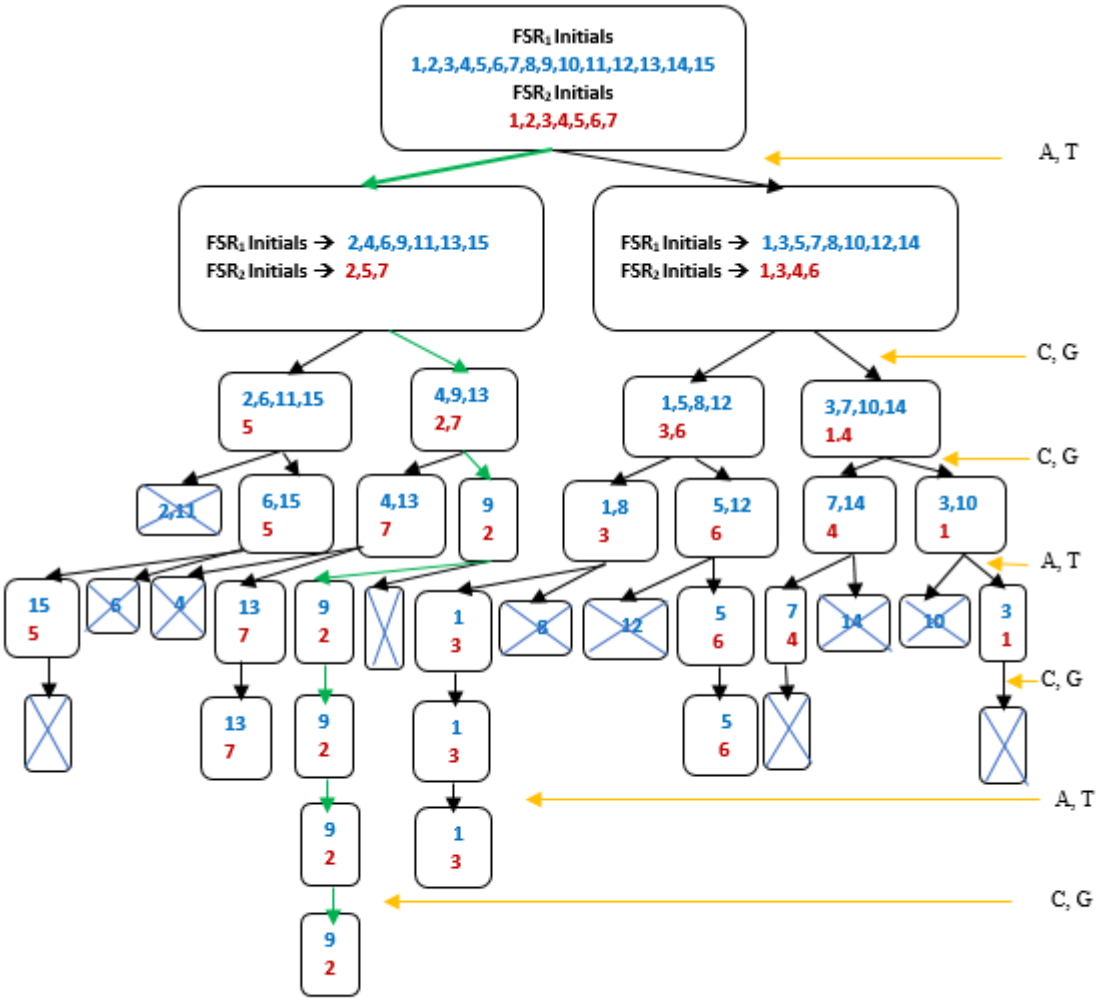
4 Algorithm Results

4.1 Experiment-1

Let us demonstrate how the proposed algorithm works by providing further clarification on its stages, and explaining how it can be used to arrive at the correct solution for attacking. Additionally, we will compare its time and storage complexity to similar methods of attacking.

We will use a simple example to apply the concepts and processes that the algorithm has come up with. Generator's description: No. of LFSR=2, Length of LFSRs are 4,3, Feedback of LFSRs = (1,4)(1,3) ,LFSRs output =feedback bits , Initials of LFSRs= 1001,010.

Keystream10 bits: 0 1 1 0 1 0 1 0 0 1, Sequence of Genetic Bases: A, T - C, G - C, G - A, T - C, G - A, T - C, G - A, T - A, T - C, G. (Remember that, the real GB sequence is A-C-C-T-G-T-G-A-T-C). Figure 3 displays the implementation output based on the algorithm steps for both phases. The green paths are the genetic base branches that lead to the correct solution. The rectangles contain the solutions that match the genetic bases, and they disappear once they are empty. However, the rectangle with the correct solution will remain until the last step of the two genetic bases gathering. The correct solution is 9,2, with the actual GBs sequence A, C, C, T, G, T, G, A, T, C, which represents the keystream 0, 1, 1, 0, 1, 0, 1, 0, 0, 1. Figure 5, shows the possible paths to reach the correct solution.



The path that sets the true initial values (9,2) is A,C,C,T,G,T,G. As an example, we need 7 KS bits to determine the exactly one correct value of the initial

Figure 5: The possible paths to reach the correct solution of the experiment no. 1.

4.2 Experiment-2

In the second experiment, we adopted the system which consists of four displacement recorders, as all its details are shown in Figure 6.

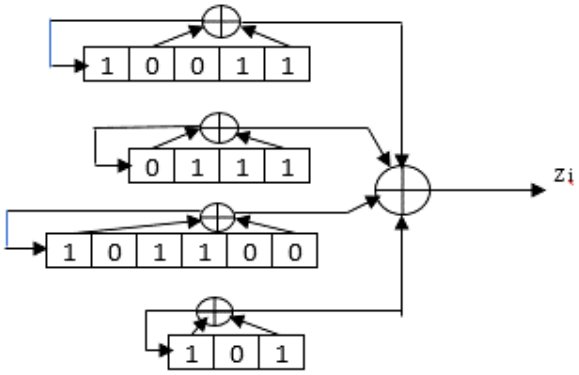


Figure 6: Details of the attacked generator of the experiment 2

In this particular search tree, the nodes at the first level (Ɛ=8) have a certain degree which increases as we go down the levels $Ɛ^2$. In this experiment, the correct solution (19,7,44,5) can only be found at the sixth level, after eliminating the nodes that cannot lead to the solution. The contents at this level hold the answer is 262,144 nodes. In Figure 7, the result of the search of the first level in the 8-degree search tree.

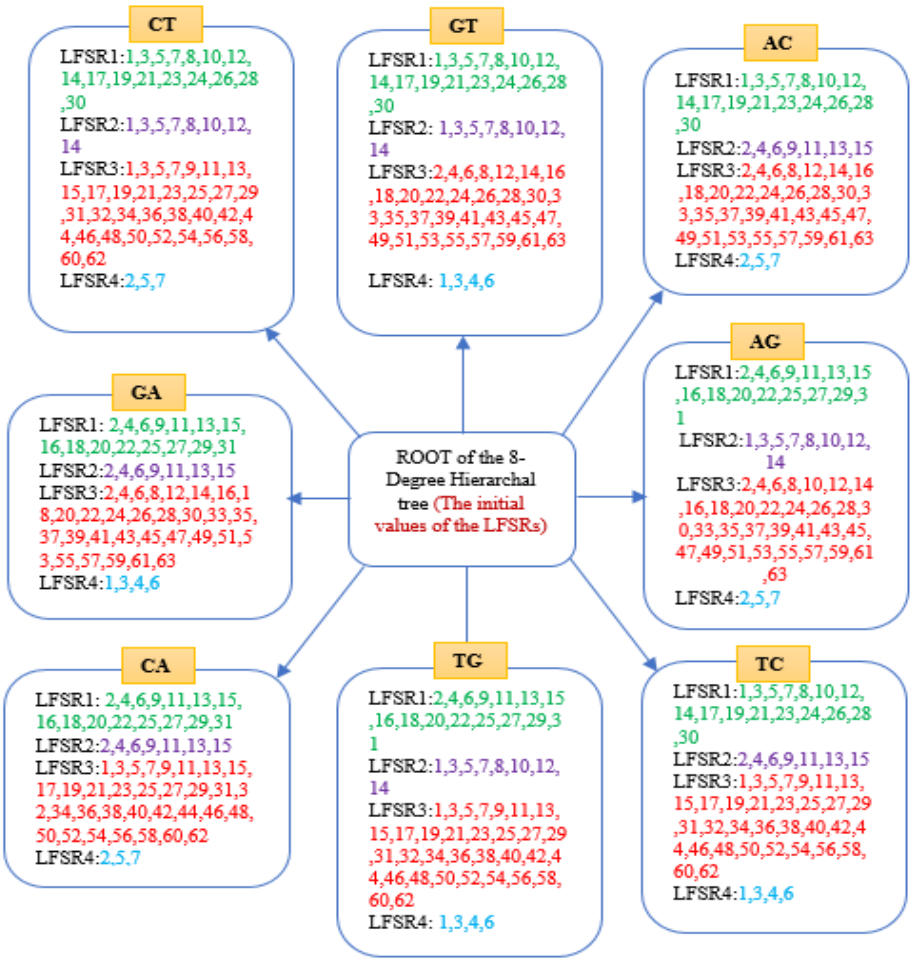


Figure 7: the result of search of the first level in the 8-degree search tree.

5 Conclusion

Emerging algorithms and methods for cryptanalysis pose a significant threat to stream cipher algorithms, which are widely used to protect confidential information in various fields. The danger lies in the fact that these algorithms and methods can be applied to real-world scenarios, making it easier for attackers to compromise the security of sensitive information. The proposed model challenges the main strength of stream key generators, their ability to resist attacks by keeping their parts cohesive. The model renders this strength useless by enabling attackers to attack each part of the generator independently, whether it's a shift register, memory, or delay. This makes it easier for attackers to compromise the security of these generators and access the confidential information they protect. We are currently experiencing a new phase in the exploration of environments other than the digital one, which can help identify weaknesses in encryption devices, specifically in stream cipher generators. Can modern encryption devices withstand the challenges posed by biological environments? The processes required to implement the model have normal specifications and do not require devices with distinctive specifications. Some important questions about the future of attacking using the proposed model

are: Can the model succeed in attacking generators of a single complex component? Will it be effective against other types of modern ciphers, such as block ciphers? Figure 8 shows the increased need for plaintext bits as the component size of the generator increases in successful attacks, which is less than the requirement for other attack algorithms of this type of cipher.

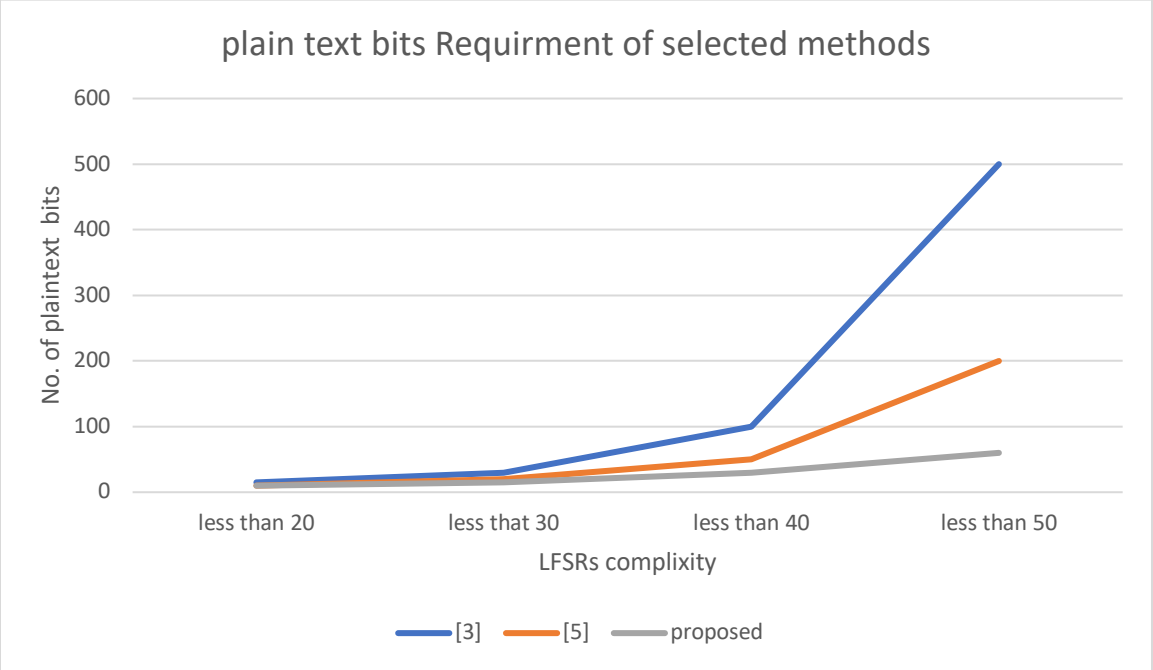


Figure 8: Increased need for plaintext bits as the component size of the generator increases in successful attacks

REFERENCES

1. Junxin;Lei Chen;and Yicong Zhou.(2020)" Cryptanalysis of a DNA-based image encryption scheme"Elsevier, Information Sciences, Vol.520, Pp:130-141, May .
2. Wei Feng; Zhentao Qin; Musheer Ahmad.(2021)" Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding ", IEEE.
3. A. S. Polenov.(2014): The Computing of NP-Complete Problems in Polynomial Time Using DNA- Logic World Applied Sciences Journal, IDOSI Publications 30(9), Pp:1188-
1192.
4. S. B. Sadkhan; B. S. Yaseen.(2018)" A DNA-Sticker Algorithm for Cryptanalysis LFSRs and NLFSRs Based Stream Cipher", International Conference on Advanced Science and Engineering, October 9-11 2018, (IEEE-ICOASE2018), University of Zakho - Duhok Polytechnic 12University, and Submitted to the IEEE Xplore Digital Library.

5. S. B. Sadkhan; B. S. Yaseen.(2019)" DB Based DNA Computer to Attack Stream Cipher", International Conference, IEEE-ICECCPCE2019, In Mosul and Erbil,13-14 February.
6. S. B. Sadkhan; B. S. Yaseen.(2019)" Hybrid Method to Implement a Parallel Search of the Cryptosystem Keys", International Conference on Advanced Science and Engineering, April 2-3 2019, (IEEE, Springer-ICOASE2019), University of Zakho - Duhok Polytechnic University, and Submitted to the IEEE Xplore Digital Library.
7. Noora Amir Abdulmehdi; Sahar Adel Kadum.(2021),' Cryptanalysis Using DNA-Sticker Algorithm', Iraqi Academics Syndicate International Conference for Pure and Applied Sciences: Conference Series 1818 (2021) 012088, Babylon-Iraq.
8. B.S. Yaseen.(2021)' Cryptanalysis of OTP Cipher Using Probabilistic DNA Computer', Design Engineering (Toronto), Issue:8, PP:10739-10748.
9. B.S.Y.(2022)' Splicing DNA Model for Unknown Stream Cipher Cryptanalysis', IEEE Conferences,2021 2nd Information Technology to Enhance E-learning and Other Application (IT-ELA).
10. Hani Z. Girgis,(2022)," MeShClust v3.0: high-quality clustering of DNA sequences using the mean shift algorithm and alignment-free identity scores", BMC Genomic, part of springer nature, Article No. 423(2022), 06 June.
11. Fereydoon azma; Mohammad ali mostafapour, Hamid Rezaei,(2012)"The application of information technology and its relationship with organizational intelligence", Elsevier, Procedia Technology1,pp:94 – 97.
12. Andrew Travers; Georgi Muskhelishivli,(2015)" DNA structure and function" the FEBS Journal, doi:10.1111/febs.13307.
13. Leslie A. Pray,(2018)" Discovery of DNA structure and function: Watson and Crick", Nature Education 1(1):100.
14. Ashish Kumar Kendhe; Hamani Agranwel,(2013)" A survey Report and various cryptanalysis techniques", International Journal of soft computing and engineering (IJSCE), Vol.3, ISSUE-2, May.
15. Sattar B. Sadkhan; Bassim S. Yaseen(2019)" DNA-based cryptanalysis: challenges, and Future trends"2019 2nd Scientific Conference of Computer Science (SCCS), IEEE-explorer.
16. Gambhir Singh; Rakesh Kumar Yadar(2019)" DNA based cryptography techniques with applications and limitations", International Journal of Engineering and Advanced Technology (IJEAT), online, Vol.-8, ISSUE-6, Aug.
17. G. Rozenberg; A. Salomaa(1999)" DNA computing: new Ideas and paradigms", International Colloquium; computer science, doi: 10.1007/3-540-48523-6_9.corpus, ID:20317046, July.
18. Christopher Swenson(2022) "Modern Cryptanalysis: Techniques for Advanced Code Breaking",1st Edition, January 23.
19. Patrick Derbez,(2023) "Tools and Algorithms for Cryptanalysis", Université Rennes 1, 2022. fftel-04013390f, HAL Id: https://hal.science/tel-04013390 Submitted on 3 Mar.
20. Jeetendra Pande(2017) " Introduction to Cyber Security (FCS)", ISBN: 978-93-84813-96-3, Published By: Uttarakhand Open University.