Security Evaluation for Stream Cipher Cryptosystem Based on Soft Computing and Theoretic Parameters

S. R. AL-Shuwaill, K. H. AL-Ibraheemi

University of Thi-Qar, College of Education for Pure Sciences, Iraq

Email: Suhamaster7@gmail.com, khalibraheemi@utq.edu.iq

Abstract. Security evaluation means an examination of a system to determine its degree of compliance with a stated security model, security standard, or specification. There are different models for security assessment, and the operation of selecting the appropriate model depends on the type of the cryptosystem. Consequently, the criteria for assessing security differ from one model to another. Information security contributes directly to increase the level of trust between users by providing an assurance of confidentiality, integrity, and availability. The main goal of this paper proposing an evaluation model of the cryptography systems. in this paper focuses the stream cipher started from its simple component LFSR and then add more than one register and using a linear feedback shift register (LFSR) with Langford arrangements to generate system to achieve randomness and complexity and evaluated based on statistical tests, information theory, soft computing (fuzzy logic), game theory. The results were acceptable and successfully passed the required tests.

1. Introduction

Cryptography is the study of mathematical techniques related to the aspects of information security requirements such as confidentiality, integrity, entity authentication, and data origin authentication. Cryptography can be considered as a set of techniques and one of the means of providing “information security”. Cryptology can be classified into three main subfields (Encryption, Cryptanalysis and Security Evaluation) [1].

Information security has significant importance to many institutions of our society: governments, military, financial, businesses, etc. Much confidential information about research, products, financial status, customers, or employees, is nowadays processed and stored on computers, or transmitted to other computers.

To define the notion of security, a third party must be set up which has access to all public information and attempts to obtain private secret information. Such a third individual is denoted as a cryptanalyst or an attacker. The notion of security can then be defined as: If an attacker cannot obtain the private secret information, a system is secure [1].

The Security evaluation domain is regarded as an important research field within the umbrella of cryptology discipline, and many of interesting experts considered it as a part of cryptanalysis.
Encryption system security standard (complexity) evaluation relies on the use of multiple methods, such as: "The Statistical parameters, Computational complexity theoretic parameters, Orthogonal Transformations, Equivalent shift register synthesis parameters, Soft computing Techniques, and Parameters based on Information theory "[2,3].

The stream cipher is an important class of encryption systems. The strong of the stream cipher system depends on the key stream generator. The generator produces pseudo-random-sequence which is must pass randomness tests.

Linear Feedback Shift Registers (LFSRs) have always received considerable attention in cryptography LFSR has wide acceptance in developing stream ciphers because of the good statistical properties, large period and low implementation costs. It used to generate the binary sequences that have simple linear complexity. However, one important drawback of LFSR is that the sequences outputted by LFSR are low complexity, and thus cryptographically insecure [4, 5, 6]. Due to the limitations of LFSR, the application of nonlinear feedback shift register (NLFSR) becomes more popular. For destroying the linearity inherent in LFSRs, three general techniques are utilized in the construction of stream ciphers: (1) a non-linear Boolean function uses on the outputs of several parallel LFSRs to form a combination generator in LFSR based stream cipher [7]. The combining function has to be carefully selected to ensure the security of the resulting scheme, for example, in order to prevent correlation attacks [8]. (2) Using a nonlinear filtering function on the contents of a single LFSR, (3) using the output of one (or more) LFSRs to control the clock of one (or more) other LFSRs [6].

1.1 Problem Statement

Research problem when proposing a specific coding system must be subject to evaluation and its validity, as these methods may fit with the proposed evaluation system, it may be computational or unconditional evaluation, or there are several ways to evaluate coding systems of all kinds. Therefore, some methods and techniques must measure the viability of a cryptographic algorithm before it can be used.

2. Background

2.1. Primitive polynomial

Theorem (1): Every polynomial f(x) with coefficients in GF (2) having f(0) = 1 divides x^m + 1 for some m. The smallest m for which this is true is called the period of f(x) [9].

Theorem (2): An irreducible polynomial of degree n has a period which divides 2^n – 1. In particular, an irreducible polynomial of degree n whose period is 2^n – 1 is a primitive polynomial [9].

2.2. Langford arrangements

Definition 1. (Arrange the numbers 11223344 ... gg in a sequence such that between equal numbers h there are exactly h other numbers. This type of arrangement of numbers is known as a Langford arrangement. Example 1. For g = 4 and g = 8, the Langford arrangements are 41312432 and 6751814657342832, respectively)[10].

Definition 2. Let (s_l)_{i=0}^{∞} be the sequence over f_q generated by a primitive LFSR of order 2g, where g is a positive integer. Suppose there exists a Langford arrangement for the number g and let k and r, respectively, denote the left and right positions of the number k in the Langford arrangement of g from the left. We define a sequence (s_l)_{i=0}^{∞} over f_q obtained from (z_l)_{i=0}^{∞} by the following recurrence relation
\[ z_i = \sum_{k=1}^{g} s2_g + i - L_k s2_{g+i} - r_k, \quad i = 0, 1, ... \]  \hspace{1cm} (1)

The equation (1) is called a nonlinearly filtered primitive LFSR based on a Langford arrangement of order \( n \) over \( f_q \), while the sequence \( \langle z_i \rangle_{i=0}^{\infty} \) is referred to as the sequence generated by the nonlinearly filtered primitive LFSR based on a Langford arrangement.

2.3. Statistical Tests

The generated Key stream will be tested using the five of following simple statistical tests (frequency test, serial test, poker test, Run test and Autocorrelation test) [9, 11, 12]. The test values must not exceed the threshold limit for each test. The threshold values for \( x_1, x_2, x_3, x_4 \) and \( x_5 \) are 3.8415, 5.9915, 14.0671, 9.4877 and 1.96, respectively. In order for the binary string that use as a key to be successful in the test, the computed value of a specific test must be less than or equal to corresponding threshold value.

2.4. Shannon’s criteria Information theory

- Entropy is an "measure of the uncertainty" of the outcome of an event. Thus Entropy is defined as: [9].
  \[ H(X) = -\sum_{i=1}^{n} P[X = i] \log P[X = i] \] \hspace{1cm} (2)

- joint entropy of plain and cipher \( H(X,Y) \): is a mathematical formula to measure the amount of joint information by observing variables \( X \) and \( Y \). (i.e. the number of bits is required to encode plain and cipher) [9].
  \[ H(X,Y) = -\sum_{i=1}^{m} \sum_{j=1}^{n} r_{i, j} \log r_{i, j} \] \hspace{1cm} (3)

- Conditional entropy of plain given cipher \( H(X|Y) \): is a mathematical formula to measure the amount of uncertainty about plain by observing variable \( Y \). (i.e. number of bits is required to encode disclosed elements of plain after cipher has been observed) [9].
  \[ H(X|Y) = -\sum_{j=1}^{n} Pr[Y = y_j] H(X|y_j) \] \hspace{1cm} (4)

2.5. Game theory

A game is an event between two or more people that ultimately compete for a reward. Games are played by anyone consciously or unknowingly on a regular basis. At the end of the game, each player has a range of strategies and each player has a pay-off. It is claimed that the player with the higher pay-off is the game-winner. In the different fields, game theory has been applied, including banking, human security, auction, economics, biological science, engineering, military, equipment/installation security, where there are limited resources and differing failure levels. [13, 14, 15, 16]. Triangular game[17,18] is a finite two-persons non-zero game, its payoff is represented by matrix game. Triangular game is nonsingular matrix, i.e. game \( A \) must be square \( n \times n \), \( A \) has inverse since its determinant is non-zero. This game submits to the indifference principle. This game is represented by triangular matrix with zeros above or below the main diagonal. Each of players has \( n \) strategies. Player1 has \( p_n \) strategies. Player2 has \( q_n \) strategies. to solve game according to the following equations are computed in theorem(3) [19].

Theorem (3): consider a game matrix \( A \) with \( m \times n \), the value of the game \( V \). Let any optimal strategy for player1 be \( p = (p_1, \ldots, p_m)^T \) and any optimal strategy for player2 be \( q = (q_1, \ldots, q_n)^T \), Then
\[ \sum_{i=1}^{n} a_{i} q_{i} = V, \text{ for all } i \text{ for which } p_{i} > 0 \] \hspace{1cm} (5)

And \[ \sum_{i=1}^{m} p_{i} a_{ij} = V, \text{ for all } j \text{ for which } q_{j} > 0 \] \hspace{1cm} (6)
2.6. Fuzzy logic theory

Fuzzy logic is a multi-value logic that, by Fuzzy variables, expresses complex models and the rules are simple and understandable and careful not to be accurate in the case. And take every value within the closed period [0 1], which corresponds to the degree of truth expressed in the fuzzy format, based on the principles of fuzzy sets as the real value of the variable [20]. The proposed will be evaluated using fuzzy logic. The fuzzification of input variables is based on two major elements (entropy H(K) key stream, conditional entropy H(X|Y)) in the decision layer of the model. The design is based on the Mamdani style inference system which is very good for the representation of human reasoning and effective analysis. The aim of this work is to assess the uncertain depending on the entropy of a key sequence by using fuzzy logic instead of human reasoning. The implementation is done using the fuzzy logic tool of MATLAB (R2018b), shown figure 4 [21].

3. Proposed security evaluations models:

In this paper, four models were proposed to assess the security of stream cipher; these models are statistical analysis, information theory, fuzzy logic, and game theory. The proposed models were applied to the LFSR which is a simple component of stream cipher key generator and two cases are considered.

1. LFSR with Langford arrangements figure (1).
2. A combination of LFSR’s with nonlinear function figure (2).

Langford arrangements created using Algorithm 1.

In the second case the lengths of registers are relatively primes in pairwise to insure a maximum period to the generated sequence which equal to LCM \( 2^{r_1} - 1, 2^{r_2} - 1, \ldots, 2^{r_n} - 1 \) where \( r_1 \) Length of LFSR\#1 , \( r_2 \) Length of LFSR\#2 , \ldots , Length of LFSR\#n , respectively, chosen three-quarters of the registers are taken and linked each pair of the registers are entered into the logical function (AND). While the other registers that are not linked with the first group are linked by the XOR function, and its output is added to the output of the first group using XOR to generate a binary sequence. Algorithm 2 , is explained the steps of nonlinear function construction.
Algorithm (1) LFSR with Langford arrangements
Input: n (register length).
Output: K key sequence corresponding to Langford connection.
Begin:
Step1: set length of LFSR to (n pairs of stages)
Step2: for I = 1 to n
    m (positions) = \( \frac{1}{2} \times (n) \) Length of Langford Arrangements
    WL = multiply (AND) Lang[i] with Lang[m]    L = number of Langford pairs
    Where Lang[i] = Lang[m]
    the products are then added to create a new (XORed) sequence
    \( K = (XOR (W(1), W(L)) \)
End

Algorithm (2) combining LFSR with nonlinear function
Input: N, number of registers with length L.
Output: K, key sequence
Begin:
Step1: Enter the number of registers
Step2: find GCD between the lengths
    if GCD(L1, L2, ..., LN) = 1 then
    Li = LSFRValue.
    For I = 1 to N
        S = (3/4)* N,
        Re = (N-S)
        S1 = Li (1) AND Li(S)
        S2 = S1 XOR Re
        K = S2
    Else
        Go to step 1
End
After the key generation, the plain text encryption process is done to obtain the cipher text.
Cipher text = plaintext XOR key sequence
4. Experimental Results

Case study 1:

Single LFSR with Langford arrangements: A linear feedback shift register considers a basic component of the stream cipher. r stage LFSR with primitive connection polynomial achieve $2^r - 1$ as a period and the generated sequence by this register has a good randomness properties. The drawback of single LFSR is simple complexity. Thus it is not possible to adopt it individually by cryptography process, so used with Langford arrangements to increase its complexity in the case study 1 the following are considered:

a) Primitive connection polynomial of degree 8, $f(x) = x^8 + x^7 + x^5 + x^3 + 1$.

b) Initial value 11010100.

c) Langford arrangement 23421314, and the number of multipliers n=4.

According to above the connection of LFSR with Langford arrangements. As follows in figure (3).

4.1. Game theory

Triangular game, one of the games in game theory showed in algorithm (3).

Algorithm (3) Triangular game theory with Shannon’s criteria

Input : (C), plaintext , (k) , key sequence , (cy) , cipher text.
Output: (V) value of the game, (A), (B), player’s strategies respectively.

Begin
Step1 : computed $H(C)$ , $H(k)$ , $H(cy)$, $H(C | cy)$. according to (2),(3),(4)
Step2: include Shannon’s entropies in triangular matrix.
Step3: solve and compute the game V and (A, B) according to equations (5),(6)
end

Now, all the required Shannon’s entropies related to LFSR cryptosystem are computed. The next step is to include these entropies in triangular game. This game is represented by triangular matrix, with zeros above or below the main diagonal. Each player has n strategies. Player1 has $p_n$ strategies and Player2 has $q_n$ strategies as illustrated in Table (1).
Table (1): Triangular Game with Shannon’s Entropies

| A Player | H(cy) | -H(C|cy) | H(k) | -H(C) |
|----------|-------|---------|------|-------|
| B Player2 | H(cy) | -H(C|cy) | H(k) | -H(C) |

Equations (10) and (11), are used to solve the Triangular game of LFSR with Langford arrangements, combination LFSR with nonlinear function and the solution will be in table (5), table (9).

4.2. Fuzzy logic

- The input to the fuzzy logic are:
  - Entropy the of a set of binary sequence identified as:
    - First set: 'H1 (k)' entropy v. good: 'trimf', [0 0.05 0.1]
    - Second set: 'H2 (k)' entropy good: 'trimf', [0.05 0.25 0.44]
    - Third set: 'H3 (k)': 'trimf', [0.25 0.45 0.65]
    - Fourth set: 'H4(k)': 'trimf', [0.45 0.75 1.114 1.291]
  - Conditional entropy of a set of binary sequence, which has a range between [0 1] it can be represented by four membership, the conditional entropy of key stream value can be divided to four sets (or more, depending on the designer decision and the resulting values from the calculation of the entropy) can be represented as:
    - First set: 'cond1': 'trimf', [0 0.1 0.2]
    - Second set: 'cond2': 'trimf', [0.1 0.2 0.3]
    - Third set: 'cond3': 'trimf', [0.25 0.45 0.58]
    - Fourth set: 'cond4': 'trimf', [0.5 0.75 1.114 1.291]
- The output to the fuzzy logic of this variable are represented by the following sets:
  - Range= [0 10]
    - First set 'v.bad': 'trimf', [0 1 2]
    - Second set 'bad': 'trimf', [1.5 2.5 4]
    - Third set 'good': 'trimf', [3.5 5 6.5]
    - Fourth set 'v.good': 'smf', [5.435 6.965]

The results of LFSR with Langford arrangements, combination LFSR with nonlinear function shown in table (6), table (10).

Case study 2
The model consists of four LFSR’s each register with a primitive connection polynomial as shown in Table 2.

| LFSR number | LFSR Length | Connection function | Initial state |
|-------------|-------------|---------------------|--------------|
| 1           | 7           | $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$ | 1111110 |
| 2           | 5           | $x^5 + x^4 + x^3 + x + 1$ | 11101 |
| 3           | 4           | $x^4 + x^3 + 1$ | 1100 |
| 4           | 3           | $x^3 + x + 1$ | 101 |
According to the proposed model, the nonlinear connection function will be built based on what is mentioned in the algorithm 2 of the paper. Three-fourths of the registers are linked to a nonlinear function and its output added to output the other registers using XORed. Output sequence according to the following relation.

\[
\text{Connection function } = ((\text{AND } \{\text{LSFRS (N)} \ast \frac{3}{4}\} ) \text{ XOR reminder })
\]

\[
f(x) = ((L1 \oplus L2 \oplus L4) \oplus L3)
\]

5. Results of proposed security evaluation model:

The results of computing statistical tests, Shannon’s Criteria (Entropy plaintext, Entropy key stream, Entropy cipher text, joint entropy and conditional entropy), Triangular game and fuzzy logic of two way different.

Case study 1 (LFSR with Langford arrangements) are displayed in Table (3), Table (4), Table (5), and Table (6).

- The generated sequence achieved acceptance results and passed statistical tests. As shown in Table 3.

| LFSR+ Langford arrangements | Frequency test | Serial test | Poker test | Run test | Autocorrelation test |
|-----------------------------|----------------|-------------|------------|----------|---------------------|
| Key stream                  | 1.1250         | 1.2293      | 1.2083     | 0.9825   | -1.7132             |
| Cipher text                 | 2              | 1.5512      | 9.0833     | 1.8260   | 0.9918              |

- According to the results of the Shannon criteria implemented for Case study 1. As shown in the table (4), we note the entropy of the key and the encoded text, its value is close to zero, as is the case for conditional entropy, where entropy is a mathematical measure of the amount of information provided. As for the conditional entropy value the amount of plaintext information that is discovered by observation the cipher text. Where small entropy value and conditional entropy a good measure the strong security.

| LFSR+ Langford arrangements | Entropy plaintext H(x) | Entropy key H(k) | Entropy cipher H(y) | Joint entropy H(x,y) | Conditional entropy H(x|y) |
|----------------------------|------------------------|------------------|---------------------|----------------------|--------------------------|
| LFSR+ Langford arrangements | 0.9937                 | 0.0351           | 0.0352              | 0.0930               | 0.0039                   |

- For other evaluate used game theory and in order to have a unique value representing all the four criteria (H(Y), H(X|Y), H(K), H(X)), Triangular game is used. The results are shown in Table 8. It is clear that p4 has the highest value (0.92658) and it refers to the importance of the criteria it represents. Then p2 has second-highest value (0.036503) and it
indicates to the importance of \( H(Y), H(X|Y), H(K) \), and the same thing for \( p3 \) and \( p1 \). Also, the value of the triangular game gives a unified value for these criteria and finally indicates to the strength of a single cryptosystem.

### Table 5: Results of triangular game theory

| Cryptosystem          | Game value | \( P1,q4 \) | \( P2,q3 \) | \( P3,q2 \) | \( P4,q1 \) |
|-----------------------|------------|-------------|-------------|-------------|-------------|
| LFSR+ Langford        | 0.0011564  | 0.032894    | 0.036503    | 0.0040276   | 0.92658     |

- Two variables (entropy and conditional entropy) as input to fuzzy logic are used to determine the security of the chosen systems. From the Table 6, we notice Evaluation values equal (7.82), this means the systems acceptable and can security evaluating, in addition, the increase membership functions for entropy input and conditional entropy the results are changed and evaluation value become more accurate.

### Table 6: The Evaluation value by Fuzzy logic

| Cryptosystem          | Entropy key | Conditional entropy | Evaluation value by fuzzy logic |
|-----------------------|-------------|---------------------|---------------------------------|
| LFSR+ Langford        | 0.00351     | 0.0039              | 7.82                            |

Case study 2 (combination LFSR with nonlinear function).

The results of computing statistical tests, Shannon’s Criteria (Entropy plaintext, Entropy key stream, Entropy cipher text, joint entropy and conditional entropy), Triangular game and fuzzy logic are displayed in a table (7), table(8), table(9), table(10). The same computations in case study 1.

- The generated sequence achieved acceptance results and passed statistical tests. as shown in Table 6.

### Table 7: Statistical tests for key stream

| Combination LFSR with nonlinear function | Frequency test | Serial test | Poker test | Run test | Autocorrelation test |
|------------------------------------------|----------------|-------------|------------|----------|----------------------|
| Key stream                               | 0              | 0.6535      | 2.3333     | 2.1790   | 1.1722               |
| Cipher text                              | 0              | 0.0236      | 2.7083     | 2.6858   | -0.8115              |

- According to Shannon’s criteria, it also achieved acceptable results, as shown in the table 8
Table 8: Shannon’s Criteria Combination LFSR with Nonlinear function

| Cryptosystem                      | Entropy plaintext $H(x)$ | Entropy key $H(k)$ | Entropy cipher $H(y)$ | Joint entropy $H(x,y)$ | Conditional entropy $H(x|y)$ |
|-----------------------------------|--------------------------|-------------------|----------------------|------------------------|-----------------------------|
| Combination LFSR With nonlinear function | 0.9937                   | 0.0625            | 0.0625               | 0.0703                 | 0.0078                      |

Triangular game theory and in order to have a unique value representing all the four criteria $(H(Y), H(X|Y), H(K), H(X))$, is used. From table 9. It is clear that $p_4$ has the highest value (0.87462) and it refers to the importance of the criteria it represents. Then $p_2$ has second-highest value (0.062264) and it indicates to the importance of $(H(Y), H(X|Y), H(K))$, and the same thing for $p_3$ and $p_1$. Also, the value of the triangular game gives a unified value for these criteria and finally indicates to the strength of a single cryptosystem.

Table 9: Results of triangular game theory

| Cryptosystem                      | Game value | $P_1,q_4$ | $P_2,q_3$ | $P_3,q_2$ | $P_4,q_1$ |
|-----------------------------------|------------|-----------|-----------|-----------|-----------|
| Combination LFSR With nonlinear function | 0.0034616  | 0.055385  | 0.062264  | 0.0077336 | 0.87462   |

- From Table 10. The value of evaluation using fuzzy logic is good for the cryptography system of combination LFSR with a nonlinear function equal (6.96).

Table 10: The Evaluation value by Fuzzy logic

| Cryptosystem                      | Entropy key | Conditional entropy | Evaluation value by fuzzy logic |
|-----------------------------------|-------------|---------------------|--------------------------------|
| Combination LFSR With nonlinear function | 0.0625      | 0.0078              | 6.96                           |
6. Conclusion

The evaluation methods proposed in evaluating the security of the stream cipher system proved to be working as a single package, as we noted that in the two study cases there is no failure in both cases in all the metrics used. The four scales can be used to evaluate the most complex cryptographic systems. And work to integrate more than one evaluation model to achieve better results in terms of security assessment of different systems.

References

[1] H. V. Tilborg, “Encyclopedia of Cryptography and Security “, Eindhoven University of Technology, The Netherland, Springer Science Business Media, Inc., USA, 2005.
[2] S.B. Sadkhan, A. H. Nasef and, S. F.Jawad , Complexity Evaluation of Knapsack Crypto System using Fuzzy Set, Journal of Basrah Researches , Volume 37. Number 4 , 2011, 473-480.
[3] Y. Lu Willi Meier and Serge Vaudenay, The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption, in M. Robshaw(Ed.), (France: Springer-Verlag,2005) 97-117.
[4] Klein A. Attacks on the RC4 stream cipher. Designs Codes Cryptogr, 2008, 48: 269–286.
[5] Zhang B, Feng D G. Improved multi-pass fast correlation attacks with applications. Sci China Inf Sci, 2011, 54: 1635–1644.
[6] Golic J D. On the linear complexity of functions of periodic GF(q) sequences. IEEE Trans Inf Theory, 1989, 35: 69–75 Alfred M., Paul O., and Scott V., "Handbook of Applied Cryptography ", CRC Press, 1996.
[7] M. Robshaw, “Stream ciphers,” Tech. Rep. TR - 701, July 1994.
[8] W. Meier and O. Staffelbach, “Fast correlation attacks on certain stream ciphers,” J. Cryptol., vol. 1, no. 3, pp. 159–176, 1989.
[9] A. Menezes, P. Oorschot, and S. Vanstone, Handbook of Applied Cryptography. CRC Press,2013.
[10] Groth, E.J.: Generation of binary sequences with controllable complexity. IEEE Trans. Inform. Theory 17, 288–296 (1971).
[11] Wenbo Mao Hewlett-Packard Company, “Modern Cryptography: Theory and Practice”,Prentice Hall PTR, ISBN: 0-13-066943-1, 2003.
[12] A. Rukhin, J. Soto, J. Nechvatal, and etc., "A Statistical Test Suite for Random and pseudorandom Number Generators for Cryptographic Applications", NIST Special Publication 800-22, Revision 1a, 2010.

[13] A. Rezazadeh, L. Zhang, G. Reniers, N. Khakzad, and V. Cozzani, “Optimal patrol scheduling of hazardous pipelines using game theory,” Process Saf. Environ. Prot., vol. 109, pp. 242–256, Jul. 2017.

[14] M. L. Shing, C. C. Shing, K. L. Chen, and H. Lee, “A Game Theory Approach in Information Security Risk Study,” Ipdrr.Net, vol. 3, pp. 201–203, 2011.

[15] K.-N. Kim, M.-S. Yim, and E. Schneider, “A study of insider threat in nuclear security analysis using game theoretic modeling,” Ann. Nucl. Energy, vol. 108, pp. 301–309, Oct. 2017.

[16] M. V. Araujo, F. A. S. Marins, M. A. R. dos Santos, U. de Oliveira, and J. Muniz Junior, “Game Theory Applied in the Management of Electric and Electronic Equipment Waste in Brazil," Adv. Recycl. Waste Manag., vol. 2, no. 2, pp. 1–9, 2017.

[17] W. P Fox, “Applied Game Theory to Improve Strategic and Tactical Military Decisions,” J. Def. Manag., vol. 6, no. 2, 2016.

[18] T. S. Ferguson, Game Theory. Stanford Encycl. Philos., vol. 44, no. 1, pp. 1–33, 2010.

[19] T. S. Ferguson, “Chapter 2- Two-Person Zero-Sum Games”, from book, GAME THEORY, UCLA, 2008.

[20] L. A. Zadeh, “Fuzzy logic Toolbox”, 2001.

[21] S. Sharma and A. J. Obaid, "Mathematical modelling, analysis and design of fuzzy logic controller for the control of ventilation systems using MATLAB fuzzy logic toolbox," Journal of Interdisciplinary Mathematics, vol. 23, no. 4, pp. 843-849, 2020.