# A Comparison of Mamdani and Sugeno Fuzzy Inference Systems based on Block Cipher Evaluation

Sirwan A. Moahmmed, Prof.Dr. Sattar B. Sadkhan

***Abstract*—Models based on fuzzy inference systems (FISs) for evaluating performance of block cipher algorithms based on three metrics are present. Two types of FIS models, Mamdani FIS model and Sugeno FIS model are used for this evaluation. Fuzzy inference systems are developed for block cipher algorithms use two types fuzzy models. The results of the two type performances of fuzzy inference systems (FIS) are compared**

***Keywords*— include at least 5 keywords or phrases.**

**Keywords: Fuzzy Logic, MFIS, SFIS, Block Cipher algorithms,**

## I. Introduction

This paper includes the comparison between two types of FIS based on security evaluated of block cipher algorithms. It will highlight the valuable assets that in general, exist in a block cipher, and that are crucial to protect for the best of the system's, also comparison between two types of FIS (MFIS and SFIS) of evaluating block cipher algorithms In this paper we use three types of block cipher RC5, Blowfish and DES algorithms [2].This study describes the experiments. Firstly the chosen three block cipher algorithms evaluate secure system used two styles of FIS. Secondly the evaluate model use different types of conjunctions logic fuzzy operator in the rules. Thirdly; Comparison of MFIS and SFIS based on the case study results with (RC5 and Blowfish) in term of security levels.

## II. Block Cipher Algorithms

Practically all symmetric block encryption algorithms in current use are based on a structure referred to as a Feistel block cipher. Whenever we treated the plaintext blocks all together to generate a block of ciphertext that has the same length, we called block cipher. Usually, the size of a block size is 64 bits. It can have the same role of a stream cipher. We can also generate a ci phertext block of y1 bits from a block of plaintext of n bits by using a clock cipher. Possibility for the decryption and reversibility for the encryption are the two different plaintext blocks which can result a ciphertext block that is unique. This transformation method is known as both non-singular and reversible [3].

## III. Types of Fuzzy Interface System (FIS)

A fuzzy Interface System (FIS) is a way of mapping an input space to an output space by employing logic. Fuzzy logic is widely used due to its ability to express the vagueness and imprecise information. FIS consists of few inputs, output, set of predefined rules and defuzzification methods [3]. Two most popular FIS models i.e. Mamdani FIS (MFIS) and Sugeno FIS (SFIS) are extensively used which are briefly described in the following subsections.

### a. Mamdani Fuzzy Interface System (MFIS)

MFIS is widely known and used in developing fuzzy models .It consists of rules of the form "IF (X1 is A1)AND (X2 is B1) AND (X3 is C1) THEN Y is F ", where X1, X2, and X3 are inputs , Y is output , then A1, B1, C1, and F are linguistic terms with MFs Triangular, Trapezoidal, and Gaussian. That represents the premise and consequent parts of the rule base. The implication is applied for each rule, generally min operator representing the (AND) and (OR) logic is used for implication. Aggregation is used to unify the output of all the rules resulting in a single fuzzy set. The aggregated output function is defuzzified in a single crisp number using a defuzzification method [3]. The framework of evaluating of block cipher algorithms uses MFIS is illustrated in figure 1

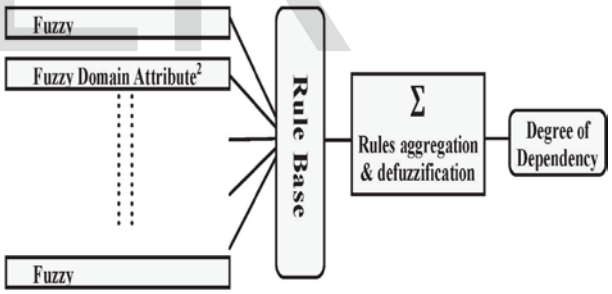


Figure 1: Structure of MFIS

### b. Sugeno Fuzzy Interface System (SFIS)

This section discusses the behavior of SFIS. It is analogous to the MFIS in several respects. The first two parts of the fuzzy interface process, are precisely identical. The one of the significant differences between MFIS and SFIS is that the SFIS output MFs are either linear or constant [4] .The SFIS rules have the following general structure:

IF (X1 IS A1) AND (X2 IS B1) AND (X3 IS C1) THEN Y =F(X1, X2, X3)

Where the input MFs for the linguistic terms A1, B1, C1, in the premise part and the output linear MF in consequent part of the SFIS rule are automatically adjusted by ANFIS

(Adaptive Neuron Fuzzy Interface System) as shown in figure 2, while in case of MFIS, the values of linguistic terms are obtained by the domain experts and evaluated on the basis of a fuzzy number scale. The ANFIS is a hybrid system that combines the potential benefits of b oth methods ANN (Artificial Neuronal Network) and FL (Fuzzy logic) [3].

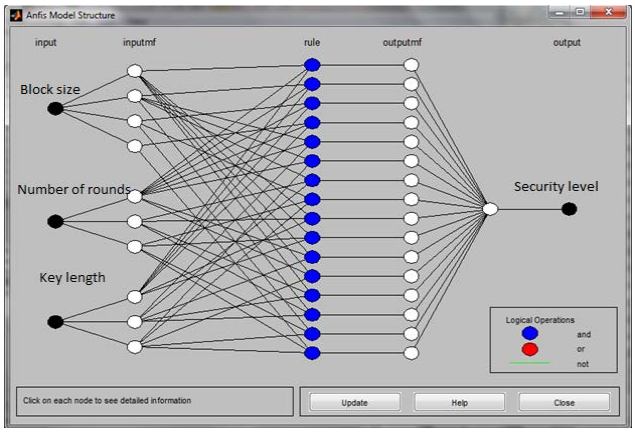


Figure 2: Model structure of ANFIS

ANFIS starts its functionality with the fuzzification of input parameters defining the MF and design of fuzzy IF-THEN rules, by effectively employing the learning capability of ANN for automatic fuzzy rule generation and self-adjustment of MFs for SFIS [3, 5]. The implication of subtractive clustering algorithm in ANFIS reduces the number of rules in Sugeno rule base by accumulating highly dented data points into a number of clusters. The SFIS having three input block size, number of rounds and key size and one output (security level) with constant output MFs f1, f2, f3, f4, f5, and their firing strength W1, W2, W3, W4, W5 can be expressed as shown in figure 3 . The final output of the system is the weighted average of all the rule outputs as illustrated in figure 3.

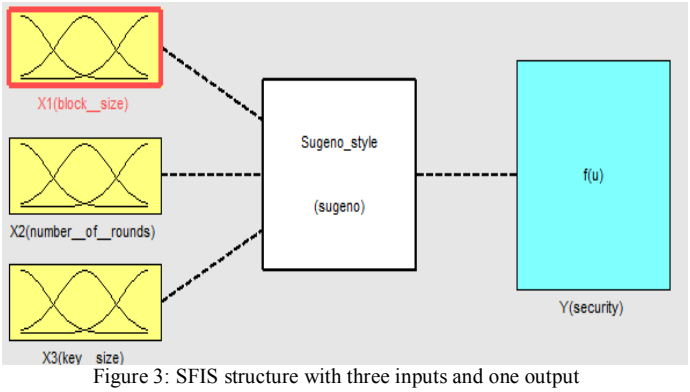


Figure 3: SFIS structure with three inputs and one output

## IV. IMPLEMENTATION

The design is implemented using the MATLAB fuzzy logic toolbox. The interfaces of the implementation are presented below:

a. FIS Types: There are two well established types of FIS: Mamdani and Sugeno As shown in Figure 4 and 5, we modelled two instances of our system using these two types of FIS to compare our results. Both systems contain the same number of inputs with the same type of membership functions and same rules but differ in the output generation process from the fuzzy inputs.

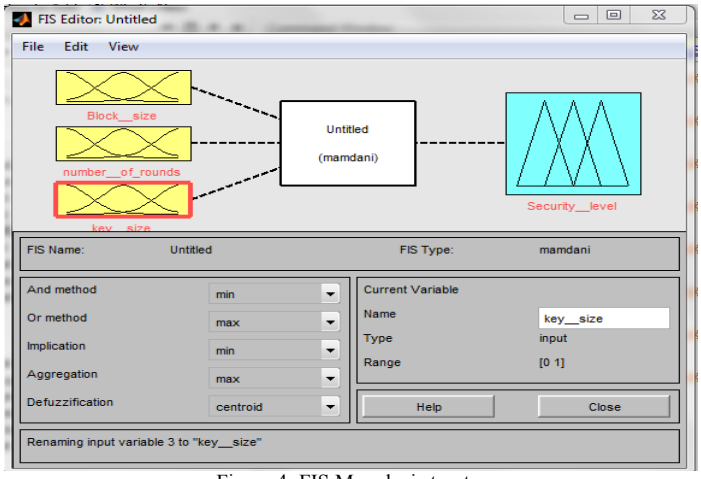


Figure 4: FIS Mamdani structure

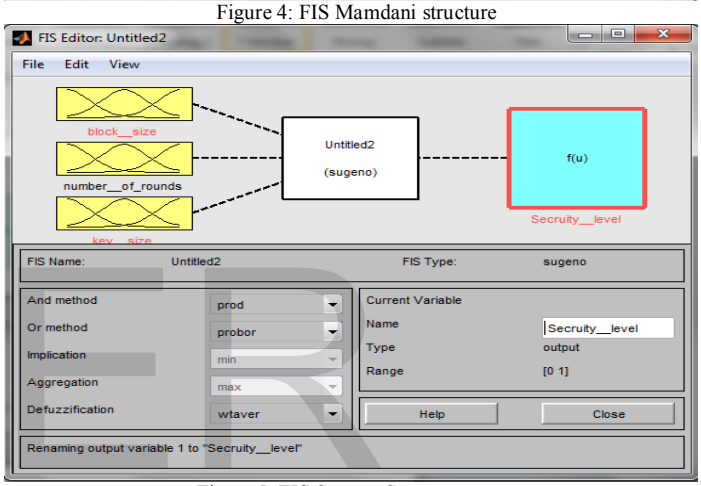


Figure 5: FIS Sugeno Structure

b. Membership function editor: The Mamdani Security level output looks like a fuzzy output. The Mamdani output is displayed in figure 6. The output has five linear memberships Functions: Very low, Low, Medium, High and Very High.

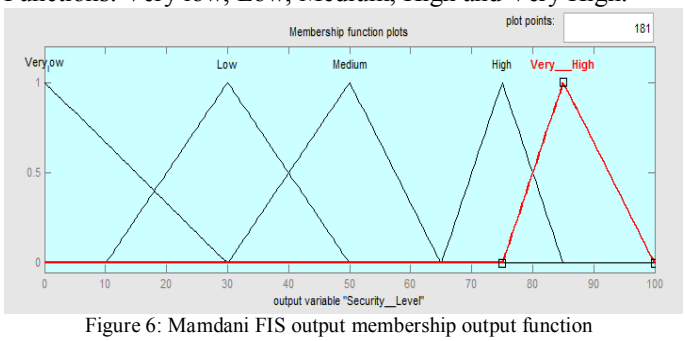


Figure 6: Mamdani FIS output membership output function

also sugeno FIS security level for the output, we divided the output into five levels and we labeled them to correspond to Mamdani's five output membership functions. The five constant membership functions along with their values are given in Table 1.

Table 1: Sugeno FIS constant output

| | |
|---|---|
| Very Low | 35 |
| Low | 50 |
| Medium | 65 |
| High | 85 |
| Very High | 100 |

It can be noted that these are output values, and the labels are just there to assist the design in MATLAB 2012a. Table 2 summarizes the differences between the Mamdani FIS and the Sugeno FIS [3].

Table2:Comparison between Mamdani FIS and Sugeno FIS

| Mamdani | Sugeno |
|---|---|
| Membership function output | Value function of output |
| Distribution of Output | Non distribution of output only 'resulting action': Mathematical combination of the output and the rules strength |
| Consequent of crisp result obtained through defuzzification of rules | Crisp result is obtained using weighted average of the rules consequent(No defuzzification) |
| The output of surface is non-continuous | The output surface is Continuous |
| It's using in MISO and MIMO systems | It's using only MISO systems |
| Expressive power and interpretable rule consequents | Loss of interpretability |
| In the system design less flexibility | In the system design more flexibility in; more parameters in the output |
| More accurate for security evaluation block cipher algorithms | Less accurate for security evaluation of block cipher algorithms |

c. Rule Viewer: The rule viewers are shown in figure7 of RC5, figure 8 o f Blowfish and figure 9 o f DES algorithm respectively shows a graphical representation of each of the variables through all the rules, a representation of the combination of t he rules and a representation of the output from the defuzzification. It also shows the crisp value for the output of the system. Each column is a variable, and each rule is a row of plots.

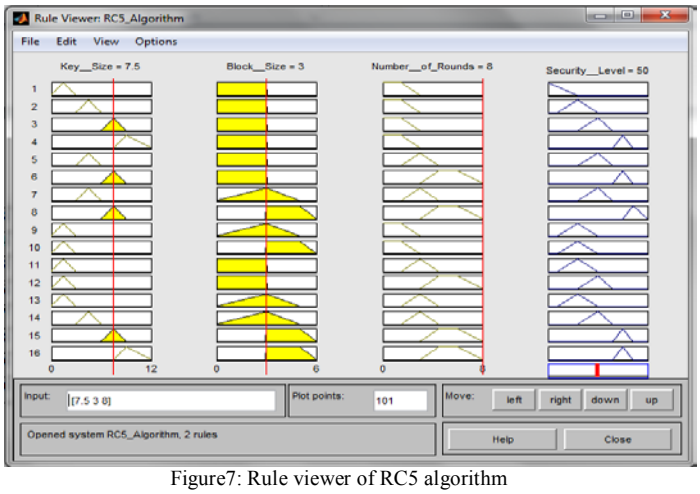


Figure7: Rule viewer of RC5 algorithm

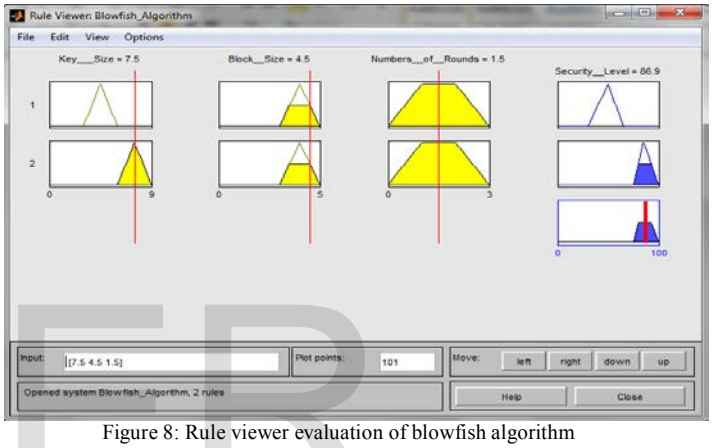


Figure 8: Rule viewer evaluation of blowfish algorithm

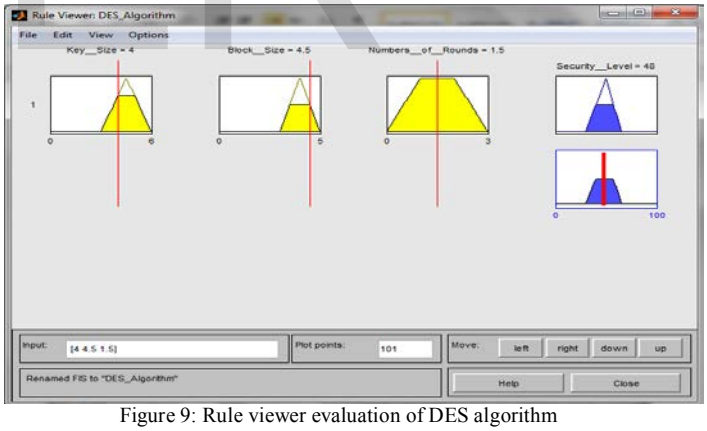


Figure 9: Rule viewer evaluation of DES algorithm

## V. Analysis and Comparison Results

a. Result of RC5 algorithm

Case one: Using Mamdani Style for FIS

1. Implementing block cipher evaluation as based on use Mamdani style of FIS in fuzzy logic, we must specify main importance parameters of the block cipher algorithms (blocks size, number of rounds and key size) and use fuzzy operator as different cases based on mamdani style and decision about security evaluation is achieved using three inputs variable and one output by 20 s tates of inputs and get output (security level) of RC5 algorithm. Then, each state needs 1.7 minutes, and time duration of this model is 48 minutes. The results of output (security level) by use (AND) and (OR) logic operator

in rules. From the results we can see used (AND) logic better than (OR) logic for modeling in fuzzy logic for security evaluation of RC5 algorithm.

Table 3: The effect of logic use Mamdani style on security level of RC5 algorithm

| States | Variable inputs | | | Output1 | Output2 |
|---|---|---|---|---|---|
| No. | Key size(bit) | Block size(bit) | Number of rounds(bit) | AND logic | OR logic |
| 1 | 1.5 | 3 | 1.5 | 21.3 | 46.1 |
| 2 | 3 | 3 | 1.5 | 50 | 46.1 |
| 3 | 4.5 | 3 | 1.5 | 30.2 | 46.1 |
| 4 | 6 | 3 | 1.5 | 50 | 46.1 |
| 5 | 7.5 | 3 | 1.5 | 48.3 | 46.1 |
| 6 | 9 | 3 | 1.5 | 75 | 46.1 |
| 7 | 10.5 | 3 | 1.5 | 75 | 46.1 |
| 8 | 12 | 3 | 1.5 | 50 | 46.1 |
| 9 | 3 | 4.5 | 1.5 | 50 | 46.1 |
| 10 | 4.5 | 6 | 1.5 | 47.8 | 38.3 |
| 11 | 6 | 4.5 | 3 | 50 | 46.1 |
| 12 | 7.5 | 6 | 3 | 48.3 | 54.8 |
| 13 | 9 | 4.5 | 4.5 | 81.7 | 54.8 |
| 14 | 10.5 | 6 | 4.5 | 50 | 66.1 |
| 15 | 12 | 4.5 | 6 | 50 | 54.8 |
| 16 | 12 | 6 | 6 | 50 | 66.1 |
| 17 | 3 | 3 | 8 | 50 | 46.1 |
| 18 | 4.5 | 4.5 | 8 | 50 | 54.8 |
| 19 | 6 | 6 | 8 | 50 | 50 |
| 20 | 7.5 | 3 | 8 | 50 | 46.1 |

b. The effective of FIS Mamdani style and fuzzy logic operator on security level based on three parameters of algorithm shows in figure (10), also mention the impact of all inputs variable (key size, block size, and number of r ounds) effect on the security level. In this figure the number of rounds is more effective than the block size on security level, and the step thirteen (13) has a high level of security (81.7 %), when the key size is 9, block size 4.5 and the number of rounds is 4.5. It means that the key size is 512 bits, the block size is 64 bits, and number of rounds is 64 bits. From these cases and results, we can prove that the fuzzy operator rule's effect on evaluation modelling, and we can see the (AND) logic operator is better than (OR) in this modelling.

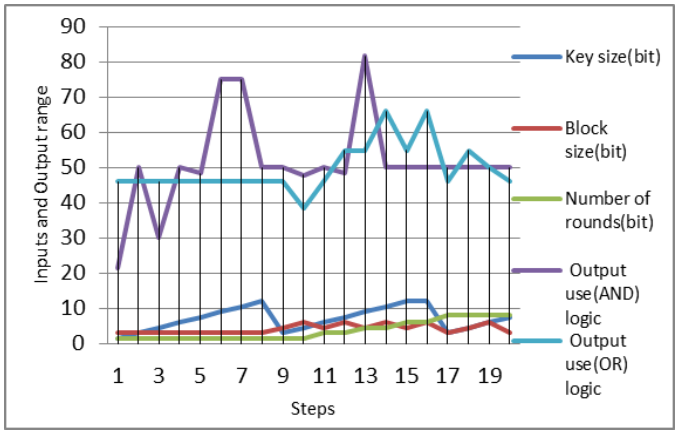


Figure 10: The effective of FIS Mamdani style and fuzzy logic operator on security level.

Case two: Using Sugeno Style for FIS

a.In this case we are use Sugeno style of FIS and two fuzzy operator (A ND) and (OR), also we are using 20 state to evaluate RC5 algorithm depend on three variable inputs, and preparing model by 35 minutes time duration of each steps 1.5 minute. In this result of this case, we notice security level depend on structure of algorithms and effect of style in evaluation in modeling of FIS as shown in table 4.

Table 4: The effect of logic types and using Sugeno on security leve of RC5 algorithm

| States | Variable inputs | | | Output1 | Output2 |
|---|---|---|---|---|---|
| No. | Key size (bit) | Block size (bit) | Number of rounds (bit) | AND logic | OR logic |
| 1 | 1.5 | 3 | 1.5 | 43.3 | 65.3 |
| 2 | 3 | 3 | 1.5 | 0.5 | 65.3 |
| 3 | 4.5 | 3 | 1.5 | 50 | 65.3 |
| 4 | 6 | 3 | 1.5 | 0.5 | 65.3 |
| 5 | 7.5 | 3 | 1.5 | 65 | 65.3 |
| 6 | 9 | 3 | 1.5 | 85 | 65.3 |
| 7 | 10.5 | 3 | 1.5 | 85 | 65.3 |
| 8 | 12 | 3 | 1.5 | 0.5 | 65.3 |
| 9 | 3 | 4.5 | 1.5 | 0.5 | 66.2 |
| 10 | 4.5 | 6 | 1.5 | 0.5 | 67.4 |
| 11 | 6 | 4.5 | 3 | 0.5 | 67.6 |
| 12 | 7.5 | 6 | 3 | 0.5 | 68.1 |
| 13 | 9 | 4.5 | 4.5 | 0.5 | 76.6 |
| 14 | 10.5 | 6 | 4.5 | 0.5 | 84.1 |
| 15 | 12 | 4.5 | 6 | 0.5 | 75.4 |
| 16 | 12 | 6 | 6 | 0.5 | 84 |
| 17 | 3 | 3 | 8 | 0.5 | 65.3 |
| 18 | 4.5 | 4.5 | 8 | 0.5 | 71.1 |
| 19 | 6 | 6 | 8 | 0.5 | 0.5 |
| 20 | 7.5 | 3 | 8 | 0.5 | 65.3 |

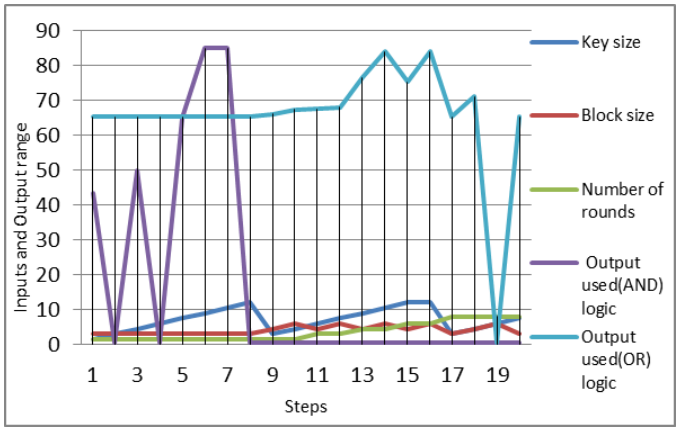


Figure 11: The effect of FIS Sugeno style and fuzzy logic operator on security level

b. Result of Blowfish Algorithm

Case One: Evaluate of Algorithm using Mamdani Style

The Blowfish algorithm has a constant number of r ounds and block size and variable range of k ey size. For this reason we have only one variable is key length to change for getting a

level of security and we have chosen five structures of the algorithm. Then we notice effect of Mamdani style of evaluating as shown in table5. Also we can see effect of types of fuzzy operator, when use (AND) we got different values of output and max level of security is step 4 (86.9%), but while use (OR) operator we got constant output (security level) is (64.3%), from this result we can prove the (AND) operator is better than (OR) used for evaluation security of block cipher algorithms.

Table 5: The effect of logic types and Mamdani style on security level of Blowfish algorithm

| States | Variable inputs | | | Output1 | Output2 |
|---|---|---|---|---|---|
| No. | Key size(bit) | Block size(bit) | Number of rounds(bit) | AND logic | OR logic |
| 1 | 3 | 4.5 | 1.5 | 50 | 64.3 |
| 2 | 4.5 | 4.5 | 1.5 | 48 | 64.3 |
| 3 | 6 | 4.5 | 1.5 | 50 | 64.3 |
| 4 | 7.5 | 4.5 | 1.5 | 86.9 | 64.3 |
| 5 | 9 | 4.5 | 1.5 | 50 | 64.3 |

Case Two: Evaluate of Algorithm using Sugeno Style

The table 6 shows the result of variable inputs and output of blowfish algorithm use two different of fuzzy operator. When we use Sugeno style in FIS get different values of security level. Also in this case we notices that the output of evaluation is constant when use (OR) logic operator, but while use (AND) logic operator got different values and max value of security level is (82.5%).

Table 6: The effect of logic types and Sugeno style on security level of Blowfish algorithm

| States | Variable inputs | | | Output1 | Output2 |
|---|---|---|---|---|---|
| No. | Key size (bit) | Block size (bit) | Number of rounds(bit) | AND logic | OR logic |
| 1 | 3 | 4.5 | 1.5 | 0.5 | 82.5 |
| 2 | 4.5 | 4.5 | 1.5 | 65 | 82.5 |
| 3 | 6 | 4.5 | 1.5 | 0.5 | 82.5 |
| 4 | 7.5 | 4.5 | 1.5 | 82.5 | 82.5 |
| 5 | 9 | 4.5 | 1.5 | 0.5 | 82.5 |

c. Results of DES algorithm

In order to verify the validity of fuzzy logic method, and then test its ability of security level for wire-wireless network, experiments were carried out over the network. In this case, the fuzzy logic method was firstly applied to set parameters input factors (training data set). Secondly the output of modeling was used as desired output (security level). Tables (7 and 8) show the results of modeling effective which are variable inputs to output by one step according to specification of an algorithm. Next there is one chosen to evaluate of DES algorithm because it has constant structure. When use type of fuzzy operator in this case a little bit different between their output results, it means that the change of the conjunction rule does not more effect on the secure evaluation. These results indicate that (OR) logic is better than (AND) logic use in fuzzy logic for evaluating DES algorithm. Also from these results (table 7 and 8), it shows that the Sugeno style is better than Mamdani. Finally the duration time of modeling is 12 minutes of use Mamdani style and 10 minutes of modeling when uses Sugeno style.

Table 7: The effect of logic types and Mamdani style at security level of DES algorithm

| States | Variable inputs | | | Output1 | Output2 |
|---|---|---|---|---|---|
| No. | Key size (bit) | Block size (bit) | Number of rounds(bit) | AND logic | OR logic |
| 1 | 4 | 4.5 | 1.5 | 48 | 48.3 |

Table 8: The effect of logic types and Sugeno style on security level of DES algorithm

| States | Variable inputs | | | Output1 | Output2 |
|---|---|---|---|---|---|
| No. | Key size (bit) | Block size (bit) | Number of rounds(bit) | AND logic | OR logic |
| 1 | 4 | 4.5 | 1.5 | 65 | 65 |

## VI. CONCLUSIONS AND FUTURE WORK

Conclusions

- The fuzzy logic tool is used to evaluate the complexity of the block cipher algorithm use of wireless network, then given parameters (key size, block work size, number of rounds, and time duration for modeling) are used to choose more secure algorithms and select secure structure of the algorithm.
- The selected encryption RC5 algorithms are used and compared with Blowfish and DES algorithm. It is found that DES algorithm consumes least encryption security level and is not flexible according to description in contrast to RC5 algorithm which consumes better than others for facility to use for evaluation which is based on fuzzy logic tools. Then the blowfish algorithm has high security level in one structure when the key size is 7.5, block size 4.5 and the number of rounds is 1.5.
- It can be said that the fuzzy logic has facility tool to evaluate the security of the information network, we make two cases of each algorithm by using two styles Mamdani and Sugeno of FIS, and two type logic operator conjunction.
- Different types of FIS styles used due to its ability in representing the ambiguity and imprecise information. This paper provides a co mparative analysis of MFIS, SFIS and used different types of fuzzy operators to evaluate the security of block ciphers.
- MFIS is implemented to evaluate the security level due to its ability to represent comprehensive linguistic information given by domain experts.
- The execution time of Sugeno is less than Mamdani of modeling.

- MFIS more accurate than SFIS In more chosen of evaluation of the block cipher algorithms.

Future Work

1- Using different methods deffuzification of MFIS and SFIS of fuzzy logic tools for block cipher algorithm evaluation and comparison between them.

2- Using different types of implication and aggregation in MFIS and SFIS of evaluating block cipher algorithms and comparisons between them.

## VII. REFERENCES

[1] Stallings William, "Cryptography and Network Security Principles and Practices", Second Edition, Printed in the United States of America, (1995).

[2] P. Ruang chaijatupon, and P. Krishnamurthy, "Encryption and power consumption in wireless LANs- N", The Third

[3] Hamam Abdelwahab and Georganas Nicolas D., " A Comparison of Mamdani and Suheno Fuzzy inference System for Evalaution the Quality of Experience of Hapto-Audio-Visual Applications", IEEE International Workshop on Haptic Audio Visual Environments and their Applications Ottawa-Canada, (2008).

[4] J.J.Jassbi, "A Comparison of Mandani and Sugeno inference Systems for a Space Faulty Detection Application", IEEE, 2008, pp. 1-8.

[5] Vibha Gaur, Anuja Soni, "Analytical inference model for prediction and customization of inter-agent dependency requirements", ACM SIGSOFT Software Engineering Notes, Volume 37 Issue 2, March 2012, pp.1-11.

IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, Sep. 27-28, 2001.