Journal of Theoretical and Applied Information Technology
10th October 2015. Vol.80. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# FUZZY SYSTEM OF ACCESS DISTRIBUTION WITHIN A COMPUTER NETWORK

**1AIGUL KAYRULAEVNA SHAIKHANOVA, 2ALEKSANDR DMITRIEVICH ZOLOTOV, 3OL'GA ALEKSANDROVNA STEPANOVA, 4MIKOLAJ PETROVICH KARPINSKI, 5LESJA ORESTOVNA DUBCHAK**

[1, 2,3]Semey State University named after Shakarim,
Glinka Street, 20a, Semey, 071410, Republic of Kazakhstan
4University of Bielsko-Biala,
Willowa Street, 2, Bielsko-Biala, 43-309, Poland.
[5] Ternopil National Economic University,
Chekhov street, 8, Ternopil, 46003, Ukraine.

E-mail: igul7@mail.ru, azol64@mail.ru, aug11@mail.ru, mkarpinski@ath.bielsko.pl, l_vasylkiv@rambler.ru

**ABSTRACT**

Continuous growth of volumes of information resources causes strict requirements to crypto protection on the processing speed of entrance data by the computer system. It is natural that for the solution of this task it is necessary to use hardware realization of known algorithms of cryptographic information protection. The method of the information protection transferred in computer networks by the choice of information encryption algorithm on the basis of fuzzy logic is offered in the article. The mechanism of fuzzy logic of Mamdani working on the min-max law is used for effective and fast reconfiguration of the server according to the current requirements of the system on the crypto strength, productivity and expenses of memory. The base of the fuzzy controller rules working on the classical mechanism of Mamdani consists of 63 rules. The offered method of fuzzy data processing is based on the division of fuzzy information processing in grade levels and operation that allowed to reduce quantity of output areas to 14 and accordingly to reduce number of operations to 4 times. The formed fuzzy system allows carrying out adequate data protection in real time, considering current state of the most computer system.

Keywords: *Time Complexity, Fuzzy System, Information Protection, Modular Exponentiation, RSA, Mamdani Method*

## 1. INTRODUCTION

The main criteria of computer system operability are high performance, optimum expenses of memory and resistance to attacks of the intruder. Any computer system can be protected from active attacks of intruder which can be found in the process thanks to known measures of security policy [22]. However, there is also possibility of passive attacks (attack of the temporary analysis or analysis of energy consumption) which can be carried out far off and therefore are difficult to find them [3], [15].

The computer system at information transfer uses network for host accessibility of clients. Such network of data transmission can be divided conditionally to protected and unprotected parts.

In the unprotected part of network clients can be casual therefore they aren't reliable for the server from the point of view of safety that is high probability of existence of the intruder. Besides, this part of network is, as a rule, not protected from malfunction owing to influences of environment and is open for carrying out all types of modern attacks to realization.

In the protected part of network clients are considered reliable and, thanks to security policy, existence of the internal intruder is excluded. However in this part of network nevertheless there is possibility of carrying out passive attack of the temporary analysis [22]. Clients of network are known to the server on the IP address and, considering "experience" of network usage, have the trust level where it is possible to set malfunction probability by transfer of information packages. So, if the client is new to this system or has very low

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

trust level, so necessary level of resistance to the temporary analysis has to be maximum, that is equal, for example, 1. On the contrary, client with very high trust level stability value can aspire to that will provide increase the system processing speed. The command subsystem of the server submits data on the most computer system that is admissible expenses of memory and necessary performance level on the information processing block [18], [24].

For information protection in network it is necessary to choose optimum method of exponentiation on the module for implementation of information encryption or carrying out authentication of the client by means of spread crypto algorithm of RSA at present. This problem is solved by the information processing block formed on the basis of fuzzy logic, namely on the mechanism of fuzzy conclusion of Mamdani [19]. It processes entrance values of productivity, expenses of memory and resistance to the temporary analysis and represents optimum method of modular exponentiation in each case on the command subsystem of the server which in turn, it is applied to information encryption. The main advantage of this block is that it works in real time that provides higher stability of system from attacks of the intruder as he will not know authentically algorithm of encryption [4], [14]. The information processing block on the basis of fuzzy logic is basis of system of computer system protection. On its entrance arrive criteria of choice of modular exponentiation method, among which necessary level of resistance to the temporary analysis R, productivity of cryptosystem R and admissible expenses of memory server M. Entrance fuzzy data are processed by the subsystem of optimum choice of exponentiation method on the module on the basis of the mechanism of fuzzy conclusion on Mamdani mechanism. The exit of the information processing block is modular exponentiation method that provides optimum configuration of protection system concerning values of entrance criteria of choice.

## 2. METHODS

The application of means Fuzzy Logic Toolbox of the MATLAB7.7.0 environment (R2008b) [11], it is possible to form fuzzy system of optimum choice of modular exponentiation method (method) depending on values of performance (performance), resistance to the temporary analysis (resistance) and admissible expenses of memory (memory) [10].

As a binary method it is possible to use a binary method with any direction of reading of bits as they have identical resistance to attack of the temporary analysis, and their productivity is almost identical.

Values of membership functions of the input variables resistance and memory it is set by trapezoid function and the input variables performance as bell shaped function [19].

Membership function of output method is set by triangular form, and in this case takes place the case of symmetric triangular membership function [7], [13].

Modeling of fuzzy conclusion is carried out on Mamdani type.

There mini-max composition of fuzzy sets is used. This mechanism includes following sequence of actions [19]:

1) fuzzification procedure: degrees of truth, i.e. the values of membership functions MFi (x) for the left-hand sides of each i-th rule (premises) are determined;

2) fuzzy inference. First the minimum level of "truncation" for the left side of each of the Ai= min (MFi (x)) rule, and then "truncated" membership function of conclusion Bi = min (Ai, Bi) are determined;

3) composition or association of obtained "truncated" functions, for which maximum composition of fuzzy sets MF(y)=max(Bi(y)) is used;

4) defuzzification. There are several methods of defuzzification. For example, centroid method. The geometric meaning of this value is the center of gravity for the curve of obtained output membership function.

## 3. RESULTS

The membership functions of variables resistance, performance and memory are divided into three intervals, each, for exact description of variables, in particular, for description of resistance to the temporary analysis is applied to the variable low $\in$ [0,0.014] designating low level of stability, middle $\in$ [0.0145,0.72] average level, high $\in$ [0.56,1] high level.

For productivity task are offered variables, high $\in$ [0,31000], middle $\in$ [27000,75000], and small $\in$ [67000,100000], answering to high, average and low levels.

Journal of Theoretical and Applied Information Technology
10th October 2015. Vol.80. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Admissible expenses of memory are set by values, small $\in$ [0.9920], middle $\in$ [9921,2.52 $\cdot$105], and big $\in$ [2.49 $\cdot$105, 5 $\cdot$105] corresponding to small, middle, big expenses.

Membership functions for output variable method can be designated by identical intervals on axis of ordinates for exact definition of the gravity center that designates fuzzy conclusion of system [19]. Binary designates binary method of modular exponentiation, beta- ary RTL and beta-ary LTR - β "from the right to the left" and "from the left to the right", accordingly, wRTL- method of the sliding window "from the right to the left", and wLTR - sliding window "from the left to the right" (figure 1).

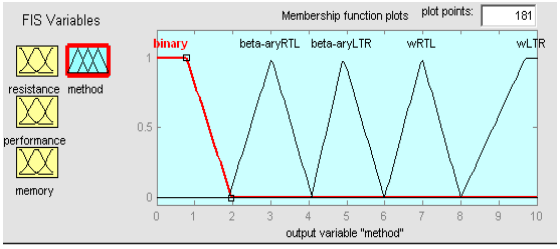



*Figure 1. The Function Of Membership Variable Method.*

The logical conclusion on the mechanism of Mamdani which finds the minimum areas in images of membership functions of entrance variables then association of the truncated areas under the maximum law is carried out and, at last there is center of gravity of final figure which abscissa is conclusion of fuzzy system is applied for creation of the offered fuzzy system. [10], [11], [14].

The knowledge base for creation of this fuzzy model consists of " rules if - that" [6], all entrance variables have three fuzzy states and one more condition of none when value of an entrance variable isn't set by system. The case when values of all entrance variables aren't set, in practice can't be put therefore the number of rules of an fuzzy conclusion of the studied system will be N = 4 · 4 · 4 -1 = 63.

System of rules of fuzzy system to choose the method of modular exponentiation

1. If (resistance is low) and (performance is small) and (memory is small) then (method is binary)
2. If (resistance is low) and (performance is small) and (memory is middle) then (method is binary)
3. If (resistance is low) and (performance is small) and (memory is big) then (method is binary)
4. If (resistance is low) and (performance is middle) and (memory is small) then (method is binary)
5. If (resistance is low) and (performance is middle) and (memory is middle) then (method is beta-aryRTL)
6. If (resistance is low) and (performance is middle) and (memory is big) then (method is wLTR)
7. If (resistance is low) and (performance is high) and (memory is small) then (method is wRTL)
8. If (resistance is low) and (performance is high) and (memory is big) then (method is beta-aryRTL)
9. If (resistance is middle) and (performance is small) and (memory is small) then (method is wRTL)
10. If (resistance is middle) and (performance is small) and (memory is middle) then (method is beta-aryRTL)
11. If (resistance is middle) and (performance is small) and (memory is big) then (method is wLTR)
12. If (resistance is middle) and (performance is middle) and (memory is small) then (method is beta-aryRTL)
13. If (resistance is middle) and (performance is middle) and (memory is middle) then (method is wLTR)
14. If (resistance is middle) and (performance is middle) and (memory is big) then (method is wLTR)
15. If (resistance is middle) and (performance is high) and (memory is small) then (method is beta-aryRTL)
16. If (resistance is middle) and (performance is high) and (memory is middle) then (method is beta-aryRTL)
17. If (resistance is middle) and (performance is high) and (memory is big) then (method is wLTR)
18. If (resistance is low) and (performance is high) and (memory is middle) then (method is beta-aryRTL)
19. If (resistance is high) and (performance is small) and (memory is small) then (method is beta-aryLTR)
20. If (resistance is high) and (performance is small) and (memory is middle) then (method is beta-aryLTR)
21. If (resistance is high) and (performance is small) and (memory is big) then (method is beta-aryLTR)
22. If (resistance is high) and (performance is middle) and (memory is small) then (method is beta-aryLTR)
23. If (resistance is high) and (performance is middle) and (memory is middle) then (method is beta-aryLTR)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

24. If (resistance is high) and (performance is middle) and (memory is big) then (method is beta-aryLTR)
25. If (resistance is high) and (performance is high) and (memory is small) then (method is beta-aryLTR)
26. If (resistance is high) and (performance is high) and (memory is middle) then (method is beta-aryLTR)
27. If (resistance is high) and (performance is high) and (memory is big) then (method is beta-aryLTR)
28. If (performance is small) and (memory is small) then (method is binary)
29. If (performance is middle) and (memory is small) then (method is binary)
30. If (performance is high) and (memory is small) then (method is binary)
31. If (performance is small) and (memory is middle) then (method is beta-aryLTR)
32. If (performance is middle) and (memory is middle) then (method is beta-aryRTL)
33. If (performance is high) and (memory is middle) then (method is beta-aryRTL)
34. If (performance is small) and (memory is big) then (method is wLTR)
35. If (performance is middle) and (memory is big) then (method is wLTR)
36. If (performance is high) and (memory is big) then (method is wLTR)
37. If (resistance is low) and (performance is small) then (method is binary)
38. If (resistance is low) and (performance is middle) then (method is wRTL)
39. If (resistance is low) and (performance is high) then (method is beta-aryRTL)
40. If (resistance is middle) and (performance is small) then (method is beta-aryRTL)
41. If (resistance is middle) and (performance is middle) then (method is beta-aryLTR)
42. If (resistance is middle) and (performance is high) then (method is beta-aryRTL)
43. If (resistance is high) and (performance is small) then (method is beta-aryLTR)
44. If (resistance is high) and (performance is middle) then (method is beta-aryLTR)
45. If (resistance is high) and (performance is high) then (method is beta-aryLTR)
46. If (performance is small) then (method is binary)
47. If (performance is middle) then (method is wLTR)
48. If (performance is high) then (method is beta-aryLTR)
49. If (resistance is low) then (method is binary)
50. If (resistance is middle) then (method is wLTR)
51. If (resistance is high) then (method is beta-aryLTR)
52. If (memory is small) then (method is binary)
53. If (memory is middle) then (method is beta-aryLTR)
54. If (memory is big) then (method is wLTR)
55. If (resistance is low) and (memory is small) then (method is binary)
56. If (resistance is low) and (memory is middle) then (method is binary)
57. If (resistance is low) and (memory is big) then (method is wLTR)
58. If (resistance is middle) and (memory is small) then (method is wLTR)
59. If (resistance is middle) and (memory is middle) then (method is wLTR)
60. If (resistance is middle) and (memory is big) then (method is wLTR)
61. If (resistance is high) and (memory is small) then (method is beta-aryLTR)
62. If (resistance is high) and (memory is middle) then (method is beta-aryLTR)
63. If (resistance is high) and (memory is big) then (method is beta-aryLTR)

The fuzzy conclusion of choice model of the modular exponentiation method formed on the basis of the set 63 rules with the current values of the resistance, performance, memory and method variables has the appearance presented on the figure 2 [6].

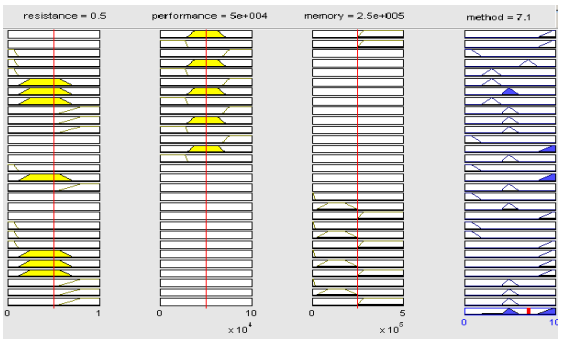
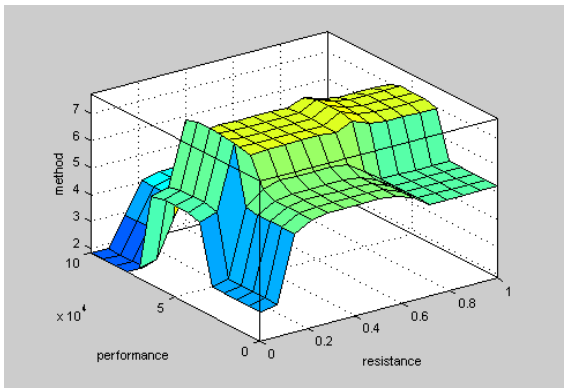


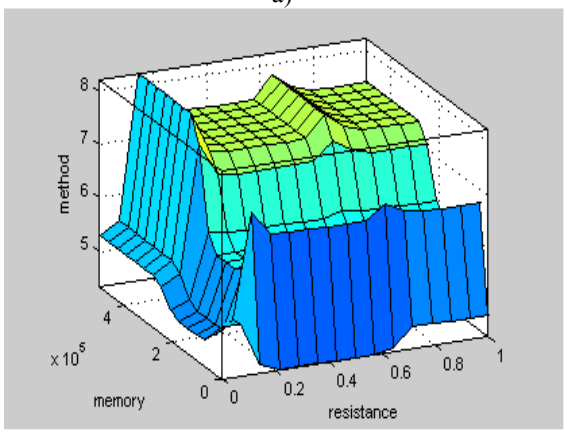

*Figure 2. Fuzzy Conclusion Of Choice Model Of The Modular Exponentiation Method.*

The surface values of the fuzzy system on the basis of Mamdani mechanism are presented on the figure 3 [6]. They confirm the correctness of the construction of the base of fuzzy inference rules.

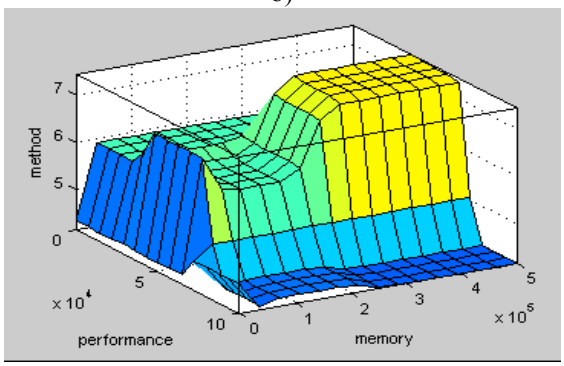
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195




a)




b)




c)

*Figure 3. The Surface Values Of Output Fuzzy System On The Basis Of Mamdani Mechanism Depending On Values:*
*A) Resistance To Temporary Analysis And Performance;*
*B) Expense Of Memory And Resistance To Temporary Analysis;*
*C) Performance And Expense Of Memory.*

## 4. DISCUSSION

The main lack of the fuzzy conclusion formed on the classical mechanism of Mamdani is that for any entrance data it is necessary to process all base of rules that is to carry out three steps. Such way of processing of fuzzy data reduces speed of system and demands big expenses of memory therefore it is worth improving the choice method of modular exponentiation method based on classical method of Mamdani which would meet requirements to processing speed.

The essence of the offered choice method of exponentiation method on the module is that processing of the entering fuzzy information is divided into grade levels and operation. During training of means of processing of fuzzy information areas of membership functions of exit for each of rules are defined.

At operation at first there is a comparison of entrance data with values of membership functions of exit in determined base of rules in memory areas where values of the mentioned membership functions of exit corresponding to each rule of fuzzy conclusion are stored. Further values of membership functions of exit are cut which exceed entrance data. Then the minimum values of the membership functions of exit received after cutting off are chosen and the corresponding figure is formed from these minimum values. After operation days of method of fuzzy data processing is search of the center of gravity of the figure received as a result of addition of the cut membership functions of exit [12], [22], [8]. In figure 4 the scheme of algorithm of realization of the offered method of processing of fuzzy data is represented.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

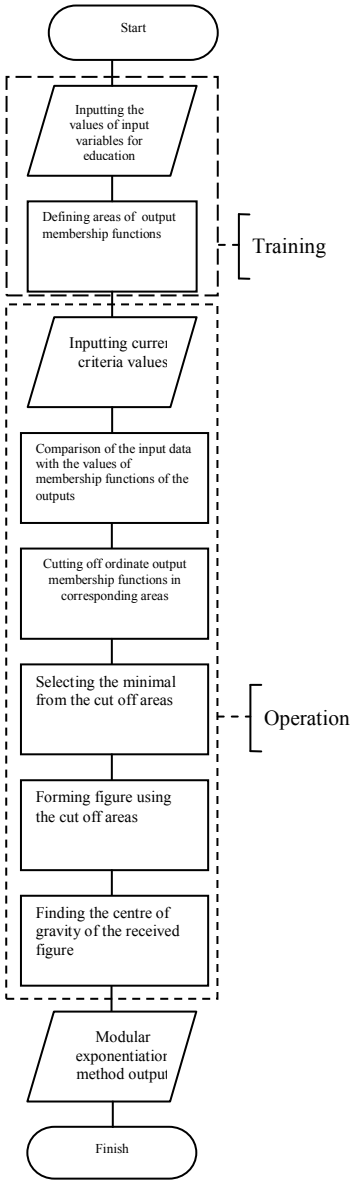



*Figure 4. The Scheme Of Realization Algorithm Of The Offered Method Of Fuzzy Data Processing*

Comparison of operations of the offered method of fuzzy information processing of classical method Mamdani at operation are provided in table 1.

*Table 1. Operations On Fuzzy Information Processing*

| №№ п/п | Transactions of an fuzzy conclusion of the classical mechanism of Mamdani | Operations of fuzzy conclusion of the offered method | |
|---|---|---|---|
| | | Coinciding operations of the offered method | New operations of the offered method |
| 1 11. | Comparison entrance data with values of membership functions of entrances | – | Comparison entrance data with values of membership functions of entrances in the ROM corresponding areas |
| 2 22. | Finding of the smallest value of membership functions of entrances on each of entrances which correspond to the base of rules | – | – |
| 3 33. | Cutting off on ordinate axis of membership functions of exit of the values exceeding the values found in item 2 | – | Cutting off on ordinate axis membership function of exit in all corresponding areas of multi channel block of memory of values which exceed the values found in item 1 |
| 4 44. | Being among the cut membership functions of exit having the maximum amplitude | – | Being among cut membership functions of exit in all corresponding areas of the multichannel block of memory having the minimum amplitude |
| 5 55. | Finding the sum found in item 4 values in the cut membership functions of exit that forms final figure | Finding the sum found in item 4 values in the cut membership functions of exit that forms final figure | – |
| 6 66. | Finding of the center of gravity of the figure received in item 5 | Finding of the center of gravity of the figure received in item 5 | – |

As it can be seen from the table 1, all operations of the offered method are close to operations of the classical mechanism of Mamdani on complexity don't exceed them. However the number of operations in the offered method is less that leads to growth of its productivity. Reduction of number of operations is caused by that at grade level (preceding an operational phase) areas of membership function of exit to each of rules are defined. Results are written down in the corresponding areas of the multichannel block of memory, from where they get out when performing operations of subitems 3, 4 of the table 1. Such

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

preliminary preparation actually also allows to avoid operations, предусмотренной provided in 2 methods of Mamdani. As temporary complexity is the main criterion of an algorithm assessment, considering the operations of fuzzy conclusion of the offered method and Mamdani mechanism described in table 1 for comparison of complexity of these algorithms it should be taken into account only incoincident operations [9]. Temporary difficulties of each operation of the considered methods of fuzzy conclusion are presented in table 2, considering the complexity calculations which are carried out in [5]. The analysis of table 2 shows that temporary complexity of the offered method of processing of fuzzy information O(n2) less, than complexity of the mechanism of fuzzy conclusion of Mamdani.

*Table 2. Temporary Complexity Of In Coincident Transactions Of Fuzzy Conclusion Of Mamdani Mechanism And The Offered Method*

| Transactions of fuzzy conclusion of the classical mechanism of Mamdani | Temporary complexity of transactions of fuzzy conclusion of Mamdani mechanism | Operations of fuzzy conclusion of the offered method | Temporary complexity of operations of fuzzy conclusion of the offered method |
|---|---|---|---|
| 1. Comparison of entrance data with values of membership function of entrances | $O(\log n)$ | 1. Comparison of entrance data with values of membership function of exits in the ROM corresponding areas | $O(\log n)$ |
| 2. Finding of the smallest value of membership function of entrances on each of entrances which correspond to base of rules | $O(n)$ | - | - |
| 3. Cutting off on ordinate axis of membership functions of the output values exceeding the value set in item 2 | $O(\log n)$ | 3. Cutting off on ordinate axis of membership functions of exit in all corresponding areas of the multichannel block of memory of values which exceed the value found in item 1 | $O(\log n)$ |
| 4.Being among the cut membership functions of exit having the maximum amplitude | $O(n^2)$ | 4.Being among cut membership functions of exit in all corresponding areas of the multichannel block of memory having the minimum amplitude | $O(n^2)$ |

At the stage of training of means of implementation of the proposed method of processing of fuzzy data, in accordance with the areas of membership functions of inputs and input data (performance - p, resistance to time analysis - r and permissible consumption of memory - m), area of the output membership functions are uniquely determined (i.e., modular exponentiation methods corresponding to these output membership functions) according to the rule base of Mamdani fuzzy inference. Obtained values corresponding to ordinates of certain output membership functions are recorded in corresponding fields of multi-channel memory block.

During the operational phase of means (Figure 5), when values of the input data are given, only areas of output membership functions corresponding to the recorded area of inputs membership functions are processed according to the rule base of fuzzy inference.

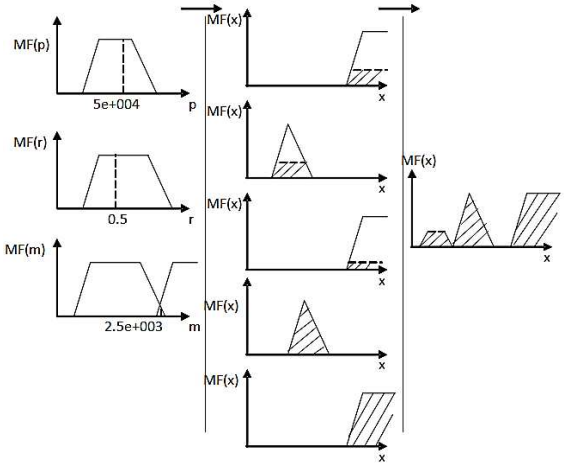



*Figure 5. Implementation Of Proposed Method Of Fuzzy Inference During The Operation*

Figure 6 shows these areas detected during the investigation of rule base of fuzzy system by means of MATLAB 7.7.0 (R2008b) [20], [2].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

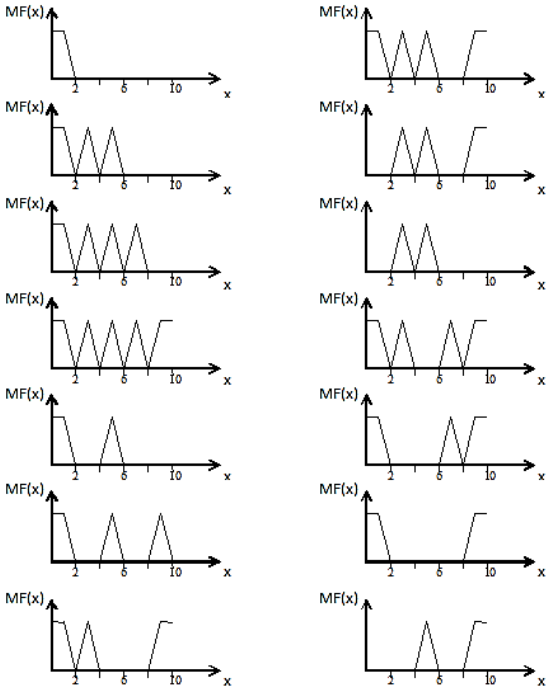



*Figure 6. Areas Of Output Membership Functions Of The Proposed Method Of Processing Of Fuzzy Data.*

Analysis of Figure 6 shows that the number of areas is 14, i.e. it decreased 4.5 times as compared to the base of 63 rules, used in classical fuzzy system based on the mechanism of Mamdani. This, in turn, accelerates the processing of fuzzy information. At the same time, output areas of the proposed fuzzy system fully reflect the output area by the classical mechanism of Mamdani fuzzy inference, which confirms the sufficiency of the operations listed in Table 1.

Thus, the proposed method of processing of fuzzy data to configure the server of computer system provides its higher performance in comparison with the classical mechanism of Mamdani fuzzy inference.

## 5. CONCLUSIONS

Thus, the offered method, according to values of temporary complexity, presented in [5], has processing speed 4 times higher, than classical (by using similar hardware equipment room of base). To reduce number of operations in the offered method and to carry out them thus as it is specified in table 1, it is possible only due to preliminary processing at grade level. Further researches can be realization of this method on PLD or PLA.

For effective and quick reconfiguration of the server in accordance with the current requirements of the system for resistance to time analysis, for performance and for consumption of memory Mamdani mechanism of fuzzy logic operating on the mini-max principle is used. The rule base of fuzzy controller operating on the classical mechanism of Mamdani, consists of 63 rules. Conducted investigations confirmed the efficiency of means of optimal selection of method of the modular exponentiation based on Mamdani fuzzy inference.

Proposed fuzzy data processing method is based on the separation of fuzzy information processing on training and operation phases, which reduced the number of output areas to 14 and correspondingly reduced 4.5 times the number of operations.

## REFERENCES:

[1] Aho A.V., Hopcroft D.E., Ullman J.D., 2001. *Data Structures and Algorithms*. Trans. from English. Moscow: Publishing House "Williams", pp. 384.

[2] Bronstein I.N., Semendyaev K.A., 1967. *Reference book on mathematics*. M.: Science. Main edition of physical and mathematical literature, pp. 608.

[3] Brumley D., Boneh D., 2005. *Remote timing attacks are practical*. Computer Networks, 48(5): 701-716.

[4] Ciet M., Feix B., Gemalto S.A. (FR), Appl. No.12/666,892; May 2, 2008; Jul.15, 2010. *Montgomery-based modular exponentiation secured against hidden channel attacks*. Patent US 2010/0177887A1, Int.Cl. H04L9/28.

[5] Constantinescu N., Simion E., 2001. *Linear Complexity Computations of Cryptographic Systems*. Telecommunications: International Conference. IEEE, Bucharest, Vol.1:85-89.

[6] Dubchak L.O, 2012. *Rule base of fuzzy system of choice of method of modular exponentiation*. Modern computer information technology (ACIT'2012). Proceedings – Ternopil, pp: 202.

[7] Gostev V.I., Skurtov S.N, Panchenko I.V., 2007. *Determination of control actions at the output of fuzzy controller under identical triangular membership function with increased slope*. Bulleten of Khmelnitsk National University. Technical sciences. Vol 5: 253-256.

[8] Hanley N., McEvoy R., Tunstall M., Whelan C., Murphy C., Marnane W.P, 2007. *Correlation Power Analysis of Large Word Sizes*. Irish Signals and Systems Conference (ISSC2007). Proceeding. Derry: 89-98.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[9] Hong S.-M., Oh S.-Y, Yoon H., 1996. *New Modular Multiplication Algorithms for Fast Modular Exponentiation.* Theory and Application of Cryptographic Techniques (EUROCRYPT'96): 15th annual international conference. Proceedings. Springer-Verlag, Germany: 166-177. http://dx.doi.org/10.1007/3-540-68339-9_15

[10] Karpinski M.P., L.O. Dubchak, N.M.Vasilkov, 2011. *Protection of information on the basis of fuzzy system.* Informatics and mathematical methods in modeling. Vol.1(3): 236-242.

[11] Lazarev Yu.F., 2011. *Simulation of dynamic systems in Matlab*. K.: NTUU «KPI», pp: 421.

[12] Messerges T.S., Dabbish E.A. Sloan R.H., 1999. *Power Analysis Attacks of Modular Exponentiation in Smartcards.* Cryptographic Hardware and Embedded Systems (CHES'99): First International Workshop. Worcester, MA, USA. Springer-Verlag Berlin Heidelberg: 144-157. http://dx.doi.org/10.1007/3-540-48059-5_14

[13] Ozyer T., Alhajj R., Barker K., 2007. *Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule pre-screening*. Journal of Network and Computer Applications. Vol. 30:99-113.

[14] Powell G.A., Wilson M.W., Truong K.Q., Curren C.P.; Mykotronx, Inc. (US), Appl. No.08/828,368; Mar.28, 1997; Aug.28, 2001. *High speed modular exponentiator*. Patent US 6,282,290B1, Int.Cl. H04K9/28.

[15] Quisquater J.-J., Koeune F, 2010. *Side Channel Attacks*. State-of-the-art regarding side channel attacks: report, pp: 47.

[16] Ros, F.J., Martinez, J.A., Ruiz, P.M., 2014. *A survey on modeling and simulation of vehicular networks: Communications, mobility, and tools*. Computer Communications. Vol. 43:1-15

[17] Ross T.J, 1995. *Fuzzy Logic with Engineering Applications*. McGraw-Hill Inc. (USA), pp:600. http://dx.doi.org/10.1016/j.comcom.2014.01.010

[18] Shaikhanova A.K., Zhangisina G.D, 2013. *Parallel calculations in the organization of the network system.* Bulleten of the Semey State University after Shakarim. Vol. 1(61): 23-31.

[19] Shtobva S.D, 2007. *Provision of accuracy and transparency of Mamdani fuzzy model during the teaching on experimental data*. Problems of management and informatics, Vol. 4: 102-114.

[20] Shumsky A.A., Shelupanov A.A., 2005. *System analysis in information security*. Textbook for university students. M.: Helios ART, pp .224

[21] Varlataya S.K., Shakhanov M.V., 2007. *The hardware and software tools and methods of information security*. Textbook. Vladivostok: Publishing FESTU, pp. 320.

[22] Vasiltsov I.V., 2009. *Special kind of attacks on cryptodevices and methods of dealing with them.* Ed. V.P. Shirochin - Kremenets: Publishing Center of KRHPI, pp: 264.

[23] Vasyltsov I.V, Son H.-K, Baek E., 2005. *Power and Fault Analysis in ECC*. Problems and Solutions. e-Smart. Conference. Sophia-Anthipolis, France, 2005:101-118.

[24] Zhangissina G., Zholymbet B., Shaikhanova A, Baiseitov D, Pavlikov R., Tursinova M., 2014. *About Parallel Computers*. International Journal of Computer Science Engineering and Information Technoligy Research. Vol. 4(2):127-132.