Research Journal of Applied Sciences, Engineering and Technology 10(9): 1082-1088, 2015
DOI: 10.19026/rjaset.10.1877
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: April 7, 2015 Accepted: April 22, 2015 Published: July 25, 2015

Research Article

Comparison of Methods of Treatment of Fuzzy Information for Distribution of Access in Computer Systems

A. Shaikhanova, G. Shangytbayeva, B. Ahmetov and R. Beisembekova
Department of Computer and Software Engineering, Kazakh National Technical University,
Named after K.I. Satpayev, Almaty, Kazakhstan

Abstract: Method of exponentiation modular for information encryption or authentication of client using the currently wide spread cryptographic algorithm RSA was considered in paper for protection of information in the network. Fuzzy system of optimal selection of method of modular exponentiation depending on the values of performance, resistance to time analysis and permissible consumption of memory was modeled. Comparative analysis of the operations of fuzzy inference by Mamdani mechanism and by proposed method was conducted.

Keywords: Fuzzy system, information protection, Mamdani method, modular exponentiation, RSA, time complexity

INTRODUCTION

The main criteria of computer system efficiency are high performance, optimal amount of memory used and resistance to malicious user attacks. Any computer system may be protected from active malicious attacks that can be detected in the process of operation due to known security policy measures (Vasiltsov, 2009). However, there is also a possibility of passive attacks (time domain analysis or energy analysis attack) that can be performed remotely and therefore are hard to detect (Brumley and Boneh, 2005; Quisquater and Koeune, 2010).

When transmitting information a computer system uses a network for customer access. This data transmission network can be conventionally divided into protected and unprotected parts.

In the unprotected part of a network clients can be random, so they are not reliable for the server from the point of view of security; that is there is a great probability of an attacker access. Moreover, this part of the network as a rule is not protected from failures due to external influences and is open to all types of modern attacks on implementation.

In the protected part of a network clients are believed to be reliable and, due to the security policy rules the existence of a malicious insider is excluded. However, in this part of the network there still remains the possibility of a passive time domain analysis attack (Vasiltsov, 2009). The network clients are known to server by an IP-address and, given the "experience" of using a network, have their level of trust where the probability of failure during the data package transfer can be assigned. Thus, if the client is new to the system, or has a very low trust level, the desired level of resistance to the time do main analysis should be maximized, i.e., equal to 1, for example.

And conversely, for a client with a very high level of trust the value of resistance can tend too, which will ensure the improvement of the system performance. The command subsystem of the server feeds to the data processing unit the data of the computer system itself, i.e., the allowable consumption of memory and the required level of performance (Shaikhanova and Zhangisina, 2013; Zhangissina *et al*., 2014).

To protect the information in the network it is necessary to choose the optimal method of exponentiation modulo for data encryption or client authentication using the currently wide spread RSA cryptographic algorithm. This problem is solved by an information handling unit built on the basis of fuzzy logic, namely, the Mamdani fuzzy inference mechanism (Shtobva, 2007). It processes the input values of performance, memory consumption and robustness to the time domain analysis; in each case it is the best method of modular exponentiation on the server command subsystem, which in its turn applies it to encrypt information. The main advantage of this unit is that it works in real time thus providing a higher robustness of the system against intruder attacks, as an intruder will not definitely know the encryption algorithm (Ciet *et al*., 2008; Powell *et al*., 1997). An information processing unit based on a fuzzy logic system is the basis of computer system protection. The criteria for selecting the method of modular exponentiation arrive at its input. The criteria include

Corresponding Author: A. Shaikhanova, Kazakh National Technical University, Named after K.I. Satpayev, Almaty 050013, Kazakhstan

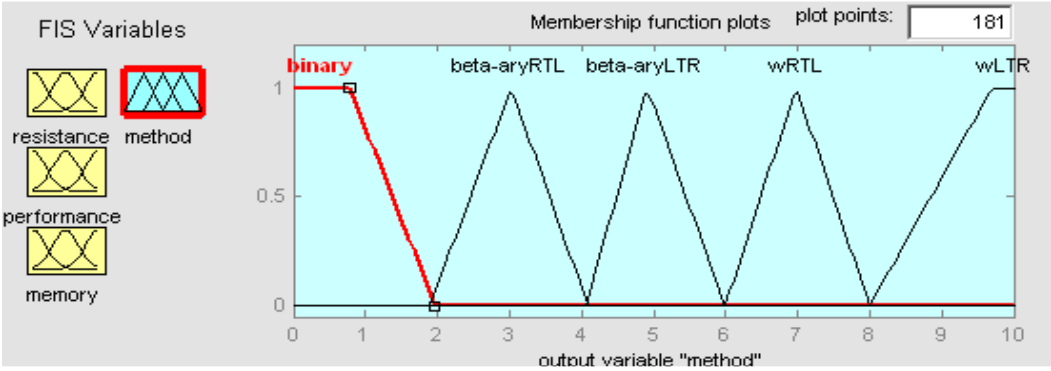


Fig. 1: Method variable membership function

the required level of resistance to the time domain analysis R, cryptosystem performance P and server memory allowable costs M. The input fuzzy data are processed by the subsystem of optimal selection of modulo exponentiation method based on the Mamdani mechanism of fuzzy inference. The output of the information processing unit is a modular exponentiation method, which provides the optimal configuration of the protection system with respect to the values of input selection criteria.

MATERIALS AND METHODS

Applying Fuzzy Logic Tool box product of MATLAB 7.7.0 (R2008b) (Lazarev, 2011) we can constructa fuzzy system for optimal selection of a method of the modular exponentiation (method) depending on the values of performance (performance), the resistance to time domain analysis (resistance) and the allowable memory consumption (memory) (Karpinski *et al*., 2011).

As the binary method may be used a binary method with any bit reading direction since they have identical resistance to the time domain analysis attack and their performance is practically the same. The values of the membership functions of the resistance and memory input variables are given by a trapezoidal function and the performance input variable-by a bell function (Shtobva, 2007).

The membership function of the method output is given by a triangular shape, at that we have the case of a symmetric triangular membership function (Gostev *et al*., 2007; Ozyer *et al*., 2007).

Fuzzy inference simulation is carried out according to the Mamdani type. The membership functions for resistance, performance and memory variables are divided into three intervals, each for a precise description of the variables, in particular, to describe the time domain analysis resistance the following variables are applied: low $\in$ (0, 0.014), indicating a low level of resistance, middle $\in$ (0.0145, 0.72) - an intermediate level and high $\in$ (0.56, 1)- a high level.

To set the performance the following variables are suggested: high $\in$ (0, 31000), middle $\in$ (27000, 75000) and small $\in$ (67000, 100000), which correspond to high, intermediate and low levels.

Allowable memory consumption is set by the values: small $\in$ (0.9920), middle $\in$ (9921, $2.52 \cdot 10^5$) and big $\in$ ($2.49 \cdot 10^5$, $5 \cdot 10^5$) corresponding to high, medium and low consumption accordingly.

The membership functions for the method output variable can be denoted by the similar ordinate intervals for accurate determination of the center of gravity, which represents the system fuzzy inference (Shtobva, 2007). Binary stands for the binary method of modular exponentiation, beta-ary RTL and beta-ary LTR β-ary "from right to left" and "from left to right" correspondingly, wRTL-sliding window method "from right to left" and wLTR-sliding window method "from left to right" (Fig. 1).

RESULTS AND DISCUSSION

For the construction of the proposed fuzzy inference system is used the logical inference according to Mamdani mechanism, which finds the minimal are as in the images of membership functions of the input variables. It is followed by the union of the truncated are as by the maximum law and, finally, detecting the center of gravity of the final figure whose abscissa is the fuzzy system inference (Karpinski *et al*., 2011; Lazarev, 2011; Powell *et al*., 1997).

The knowledge base for the construction of the fuzzy model consists of "if-then" rules (Dubchak, 2012). All the input variables have three fuzzy states and one more state, none, when the value of the input variable is not defined by the system. The case when the values of all input variables are not set cannot be applied in practice, so the number of fuzzy inference rules of the investigated system will be N = 4.4.4-1 = 63.

The fuzzy inference of the model of selecting a modular exponentiation method built on the basis of 63 set rules with the current values of resistance, performance, memory and method variables, has the form represented in Fig. 2 (Dubchak, 2012).

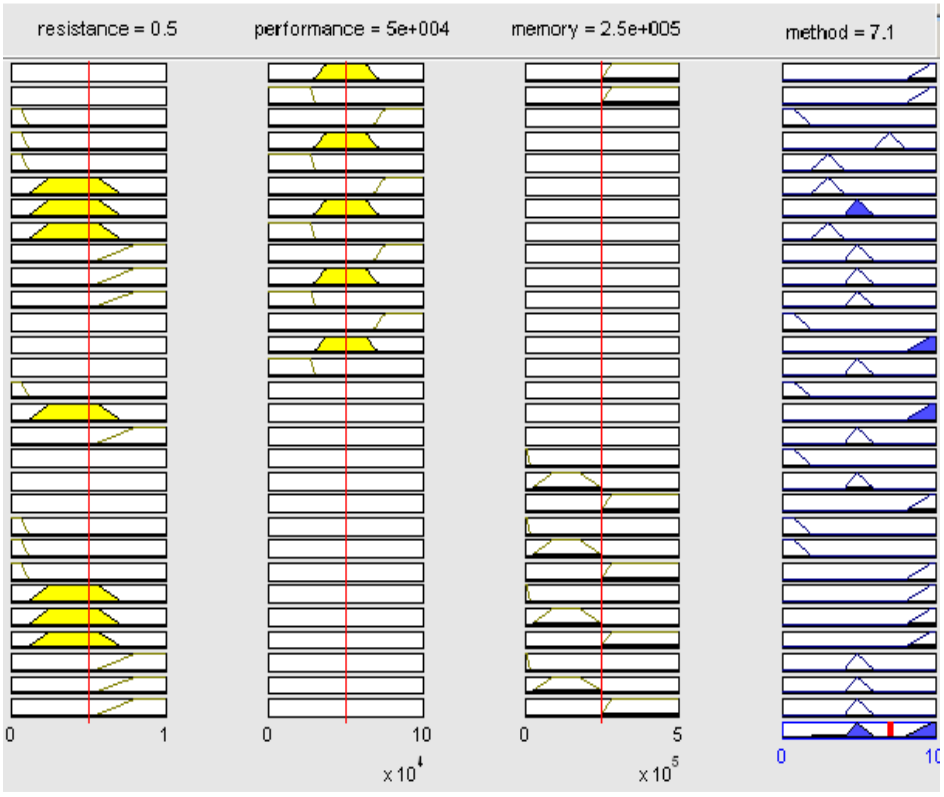


Fig. 2: The fuzzy inference of the model of selecting a modular exponentiation method

The surfaces of values of a Mamdani mechanism based fuzzy system are represented in Fig. 3 (Dubchak, 2012). They confirm the correctness of the construction of the base of fuzzy inference rules.

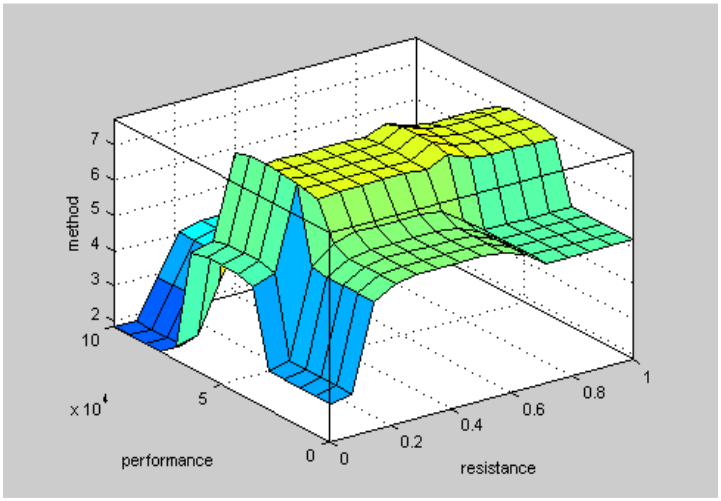
The main disadvantage of the fuzzy inference built using the classical mechanism of Mamdani is the fact that for any input data it is necessary to process the entire rule base, that is, to carry out three steps. This way of processing fuzzy data reduces system performance and requires more memory consumption. That is why we need to improve the method of choice of the modular exponentiation method based on the classical method of Mamdani, so that it would satisfy the requirements for high-speed performance (Ross, 1995; Ozyer *et al*., 2007; Ros *et al*., 2014).

The idea of the proposed selection method for the exponentiation modulo is that the processing of incoming fuzzy information is divided in to the stages of education and operation. During education of fuzzy information processing tools are identified the areas of membership functions of output for each of the rules.

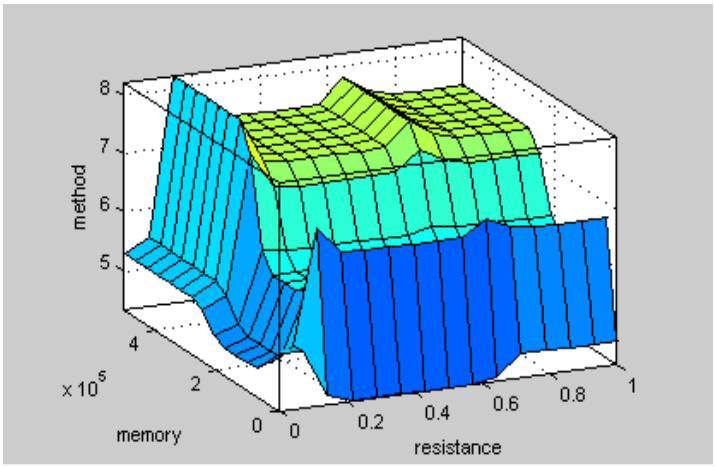
During operation first the input data is compared to the values of output membership functions in the memory areas defined by the rule base, where the values of the above mentioned output membership functions corresponding to each fuzzy inference rule are stored. Then the values of output membership functions that exceed the input data are cut off. After that the minimum values of the output membership functions received after the cut-off are selected and the corresponding figure is constructed using these minimum values. The last operation of the method of fuzzy data processing is finding the center of gravity of the figure received by adding the clipped output membership (Vasyltsov *et al*., 2005; Hanley *et al*., 2007). Figure 4 shows the diagram of the proposed method of processing fuzzy data implementation algorithm.

The comparison of operations of the proposed method of processing fuzzy information and the classical method of Mamdani during operation are shown in Table1.

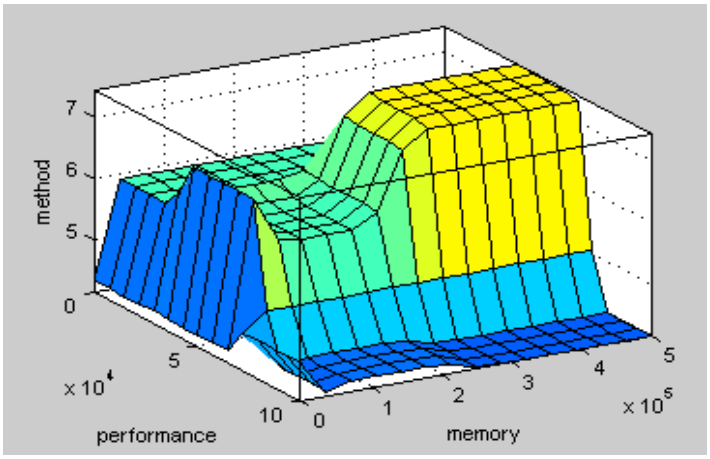
As can be seen from Table 1, all the operations of the proposed method are similar to the operations of the classical Mamdani mechanism and do not exceed them in complexity. However, the number of operations in this method is smaller, which leads to the increase of its performance. Reducing the number of operations is conditioned by the fact that during the education phase (prior to the operation phase) are identified the areas of output membership functions for each of the rules. The results are recorded in the corresponding areas of the multichannel memory storage unit where they are selected when performing operations 3 and 4 of



(a)



(b)



(c)

Fig. 3: The surfaces of values of a Mamdani mechanism based fuzzy system output depending on the values of; (a): Resistance to the time domain analysis and performance; (b): Memory consumption and resistance to the time domain analysis; (c): Performance and memory consumption

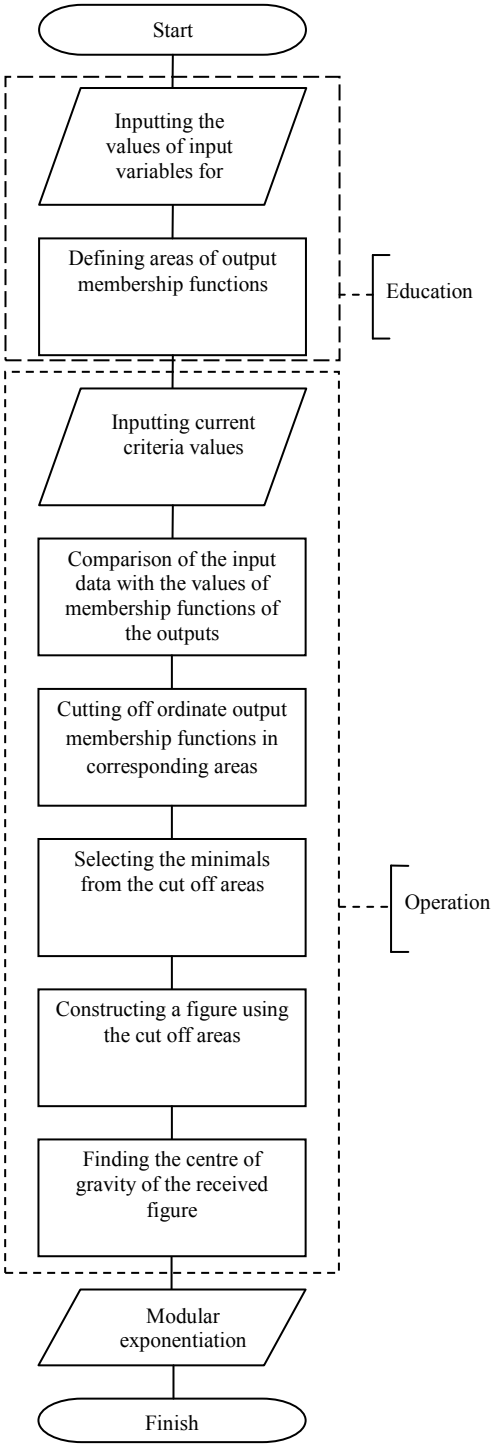


Fig. 4: Scheme of the algorithm of implementing the proposed method of processing fuzzy data

Table 1. Such an advance preparation allows avoiding the operations referred to in p.2 of Mamdani method. Since the time complexity is the main criterion for evaluating the algorithm, then considering fuzzy inference operations of the proposed method and the mechanism of Mamdani described in Table 1 for comparison of the complexity of these algorithms we should consider only non-coinciding operations (Hong *et al*., 1996). Table 2 shows the time complexity of each of the operation of the considered fuzzy inference methods taking in to account the complexity calculations carried out in (Constantinescu and Simion, 2001). The analysis of Table 2 demonstrates that the time complexity of the proposed method of processing fuzzy information is by O (n^2) less than the complexity of the Mamdani mechanism of fuzzy inference.

Table 1: Fuzzy information processing operations

No.	Fuzzy inference operations based on the classical Mamdani mechanism	Fuzzy inference operations based on the proposed method: Coincident operations of the proposed method	Fuzzy inference operations based on the proposed method: New operations of the proposed method
1.	Comparing input data to the values of input membership functions	-	Comparing input data to the values of input membership functions in the corresponding ROM areas
2.	Finding the minimal value of input membership functions for each of the inputs that corresponds to the rule base	-	-
3.	Cutting off the ordinate values of the output membership functions that exceed the values found in p.2	-	Cutting off the ordinate values of the output membership functions in all the corresponding areas of the multi-channel memory unit that exceed the values found in p.1
4.	Finding the output membership functions with the maximum amplitude among the cut-off functions	-	Finding among the cut-off output membership functions in all the corresponding areas of the multi-channel memory unit the ones with the minimum amplitude
5.	Finding the sum of the received in p.4 values of the cut-off output membership functions, which forms the final figure	Finding the sum of the received in p.4 values of the cut-off output membership functions, which forms the final figure	-
6.	Detecting the center of gravity of the figure received in p.5	Detecting the center of gravity of the figure received in p.5	-

Table 2: The time complexity of the non-coincident fuzzy inference operations according to the Mamdani mechanism and to the proposed method

Fuzzy inference operations according to the classical Mamdani mechanism	The time complexity of the fuzzy inference operations according to the classical Mamdani mechanism	Fuzzy inference operations according to the proposed method	The time complexity of the fuzzy inference operations according to the proposed method
1. Comparing input data to the input membership function values	O (logn)	1. Comparing input data to the output membership function values in the corresponding ROM areas	O (logn)
2. Finding the minimal value of input membership functions for each of the inputs that corresponds to the rule base	O (n)	-	-
3. Cutting off the ordinate values of the output membership functions that exceed the values found in p.2	O (logn)	3. Cutting off the ordinate values of the output membership functions in all the corresponding areas of the multi-channel memory unit that exceed the values found in p.1	O (logn)
4. Finding the output membership functions with the maximum amplitude among the cut-off functions	O (n^2)	4. Finding among the cut-off output membership functions in all the corresponding areas of the multi-channel memory unit the ones with the minimum amplitude	O (n)

CONCLUSION

Thus, the proposed method according to the time complexity values presented in (Constantinescu and Simion, 2001) has a 4 times higher high-speed performance than the classic one (using the analogue hardware base). Reducing the number of operations in the proposed method and performing them the way it is indicated in Table 1 is manageable only due to the preliminary processing at the education stage. Further research may be the implementation of this method in PLD or PLA.

REFERENCES

Brumley, D. and D. Boneh, 2005. Remote timing attacks are practical. Comput. Networks, 48(5): 701-716.

Ciet, M., B. Feix and S.A. Gemalto (FR), 2008. Appl. No.12/666,892; May2, 2008; Jul.15, 2010. Montgomery-based modular exponentiation secured against hidden channel attacks. Patent US2010/0177887A1, Int. Cl.H04L9/28.

Constantinescu, N. and E. Simion, 2001. Linear complexity computations of cryptographic Systems. Proceeding of IEEE International Conference on Telecommunications, Bucharest, 1: 85-89.

Dubchak, L.O., 2012. Rule base of fuzzy system of choice of method of modular exponentiation. Proceeding of Modern Computer Information Technology (ACIT'2012), Ternopil, pp: 202.

Gostev, V.I., S.N. Skurtov and I.V. Panchenko, 2007. Determination of control actions at the output of fuzzy controller under identical triangular membership function with increased slope. Bull. Khmelnitsk National Univ., Tech. sci., 5: 253-256.

Hanley, N., R. McEvoy, M. Tunstall, C. Whelan, C. Murphy and W.P. Marnane, 2007. Correlation power analysis of large word sizes. Proceeding of Irish Signals and Systems Conference (ISSC2007), Derry, pp: 89-98.

Hong, S.M., S.Y. Oh and H. Yoon, 1996. New modular multiplication algorithms for fast modular exponentiation. Proceeding of 15th Annual International Conference on Theory and Aapplication of Cryptographic Techniques (EUROCRYPT'96), Germany, pp: 166-177.

Karpinski, M.P., L.O. Dubchak and N.M. Vasilkov, 2011. Protection of information on the basis of fuzzy system. Inform. Mathe. Methods Model., 1(3): 236-242.

Lazarev, Y.F., 2011. Simulation of dynamic systems in Matlab. K: NTUU«KPI», pp: 421.

Ozyer, T., R. Alhajj and K. Barker, 2007. Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule pre-screening. J. Network Comput. Appl., 30: 99-113.

Powell, G.A., M.W. Wilson, K.Q. Truong, C.P. Curren, 1997. 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.

Quisquater, J.J. and F. Koeune, 2010. Side channel attacks. State-of-the-Art Regarding Side Channel Attacks, Report, pp: 47.

Ros, F.J., J.A. Martinez and P.M. Ruiz, 2014. A survey on modeling and simulation of vehicular networks: Communications, mobility and tools. Comput. Communi., 43: 1-15.

Ross, T.J., 1995. Fuzzy Logic with Engineering Applications. McGraw-Hill Inc., USA, pp: 600.

Shaikhanova, A.K. and G.D. Zhangisina, 2013. Parallel calculations in the organization of the network system. Bull. Semey State Univ. Shakarim, 1(61): 23-31.

Shtobva, S.D., 2007. Provision of accuracy and transparency of mamdani fuzzy model during the teaching on experimental data. Prob. Manage. Inform., 4: 102-114.

Vasiltsov, I.V., 2009. Special kind of attacks on crypto devices and methods of dealing with them. In: Shirochin-Kremenets, V.P. (Ed.): Publishing Center of KRHPI, pp: 264.

Vasyltsov, I., H.K. Son and E. Baek, 2005. Power and fault analysis in ECC. Proceeding of Problems and Solutions e-Smart Conference, Sophia-Anthipolis, France, pp: 101-118.

Zhangissina, G., B. Zholymbet, A. Shaikhanova, D. Baiseitov, R. Pavlikov and M. Tursinova, 2014. About parallel computers. Int. J. Comput. Sci. Eng. Inform. Technol. Res., 4(2): 127-132.