Access Distribution Scheme to the Computer System Based on Fuzzy Logic

A. Shaikhanova, A. Zolotov, L. Dubchak, M. Karpinski and V. Karpinskyi

Abstract This paper presents access distribution at computer system transmission of client-server data type. In order to enhance information protection fuzzy logic is applied to select the data encryption method. A server block diagram of such computer system has been developed based on the proposed fuzzy distribution of system access.

Keywords Client-server model · Fuzzy logic · Timing attack · Modular exponentiation · Resistance to side-channel attacks

1 Introduction

Client-server architecture is one of the most popular concepts in creating computer information systems. This architecture includes the following components:

A. Shaikhanova (✉) · A. Zolotov
Semey State University named after Shakarim, Semey, Kazakhstan
e-mail: igul7@mail.ru

A. Zolotov
e-mail: azol64@mail.ru

L. Dubchak
Ternopil National Economic University, Ternopil, Ukraine
e-mail: l_vasylkiv@rambler.ru

M. Karpinski
University of Bielsko-Biala, Bielsko-Biała, Poland
e-mail: mkarpinski@ath.bielsko.pl

V. Karpinskyi
The Techno Centre, Coventry University, Coventry, UK
e-mail: vkarpinskyi@gmail.com

S. Zawiślak and J. Rysiński (eds.), *Graph-Based Modelling in Engineering*,
Mechanisms and Machine Science 42, DOI 10.1007/978-3-319-39020-8_3

– back-end (preservation and processing of information);
– client side (user's instrument manual);
– network that provides interaction (exchange of information) between a client and a server.

Most of web-based systems are based on this architecture.

Such systems can be extremely varied and complex. The advantages of web-based systems based on client-server architecture are [4, 7]: minimum maintenance cost of business processes, maximum efficiency of data handling, easy maintenance, minimum cost of communication between business units, possibility of connection to the system from any computer with Internet access.

Each client of computer network is identified by its IP address and has its own "history" of using the information processing and transmission system regarding the presence of failures or data loss while transmitting ciphertext. This information is stored on a server that assigns to a user its level of access to information (Fig. 1).

However, when a violator performs the time attack or substitution of the IP-address stability of cryptosystem cannot be univocally provided [3, 4, 6].

Hundreds of thousands of network intrusions are registered during a year. However, taking under consideration that 80 % of computer crimes are not included in the official statistics because victims are afraid of publicity, which could undermine their trust of the partners and customers [12].

Modern information processing systems are represented as sophisticated software and hardware systems with specific information leakage channels accompanied with operational processing of information resources.

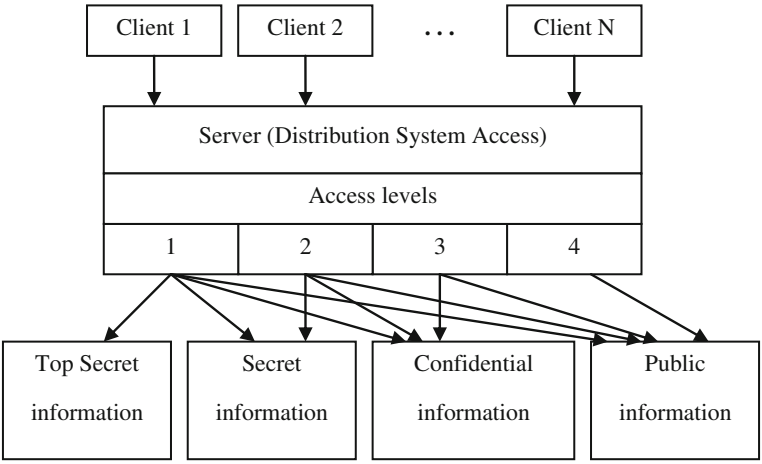

Fig. 1 Information access levels of computer system users

Thus, computer systems are exposed to a wide range of potential threats that causes necessity to anticipate a large list of functions and subsystems protection. First of all, it is necessary to protect the most informative channels of information leakage.

Overlapping problems of those channels are complicated by the fact that data protection procedures should not lead to a noticeable reduction in Computer System (CS) performance.

Since, access to information in most of CS is carried out remotely via the Internet; because of this it is essential to protect information against unauthorized access.

Threats to computer systems can be classified into nine features [4]:

1. For the purpose of threat implementation: breach of confidentiality; disturbing of the information integrity; disturbing of computer systems functioning.
2. According to the principle of the influence on the CS:
   - using a systems subject access (user, process) to the object (data file, data link, etc.);
   - using the covert channels (information transmission paths that allows for two cooperating processes to share information in a manner that disturbs the system security policy).

Interventions based on the first principle are simpler and more informative; it is easier to defend against them. Interventions based on the second principle are distinguished of level organization difficulty, lower information providing and difficulty in detection and removal.

3. The nature of the impact on CS:
   - active threat, that leads to a change of the system state and can be carried out either using the access or using both access and covered channels together;
   - passive threat, carried out by user observing of any side effects and their analysis. An example of passive impact may be a monitoring of the link between two network nodes. Passive impact does not lead to the system change. It is always associated with breach of confidentiality in the CS.
4. By reason of protection error use, this can be caused by one of the following:
   - inconsistency of security policy in real CS;
   - administrative management errors, which refers to incorrect implementation or support of security policies adopted by the CS;
   - errors in algorithms, relations between them and others that occur in the design phase of the program or set of programs. Therefore, they can be used in a wrong way, not as described in the documentation;
   - realization errors in algorithms (coding errors), links between them etc., which occur at the stage of implementation or debugging and can also be a source of undocumentation.

5. By manner of influence on the object of attack (in case of active impact):
   - direct impact on the object of attack (such actions are usually easily prevented with the help of access control);
   - impact on the system permission (including seizure of privileges);
   - mediate influence (through other users);
   - "masquerade", in that case the user assigns itself different user authorities (pretends to be it);
   - "user blindfold"—when one user is forcing another to perform required actions, where the last may not suspect that; for this purpose virus can be used (it takes appropriate action and informs the one, who brought him, about the outcome).
6. By manner of influence on CS: in interactive mode and in batch mode.
7. By object of the attack:
   - CS in general (intrusion into the system), for that purpose usually is used method of "masquerade", interception or fake password, "hacking" and access to CS through the network;
   - CS objects—data or programs, the system devices, data transmission channels;
   - CS subjects—users' processes and sub processes, frequent case of such influence is loading of malicious virus to the environment of another process and its execution on behalf of that process;
   - data transmission channels—channels, data packets transmitted by communication channels, channel monitoring and traffic analysis (message flow, substitution or message modification in communication channels and in retranslation nodes, topology and characteristics changes of the network).
8. By used tools of attack (using either standard software or specially designed programs).
9. By object state of attack. The object of attack can be in one of three states:
   - saving—impact on an object is usually carried out by using the access;
   - transmission—effect provides either access to fragments of transmitted information or monitoring using covert channels;
   - processing—user process is the target object.

There are four standard methods that you can apply to restrict the access to information in a computer system [4, 12]:

- access control (the check of IP-address of each received packet, restriction of access with passwords, application of software tools);
- extension of password protection (response to a remote call, that is checking the password by a "recall", continuous handshaking of connection—a system in which the server continually negotiates with the client computer during the connection session);

– encryption (the most popular asymmetric information security system is RSA, that enables creation of a sustainable digital signature);
– firewall (a combination of hardware and software to prevent access to information from the Internet).

These approaches do not provide a complete stability of a system since a violator can substitute an IP-address, intercept data packets that are transmitted through the communication channel and thus find out the password. Therefore to ensure the stability of a computer system that uses a client-server type network for data transfer it is necessary to consider the most dangerous attacks that can be carried out through the side channels of information leakage.

According to the ways of information interception, physical nature of data transmission channels, as well as the environment of information dissemination, the channels of leakage and interception of information can be divided into electromagnetic, electric, acoustic, cable local area networks (LANs), visual, inductive, parametric, bookmarks and viruses [8, 13].

Attacks of extraneous information leakage channels are characterized by less power than traditional attacks based on mathematical analysis of a cryptographic algorithm, but at the same time they are much more effective. Their research is presented in [2, 10]. The most dangerous attack of this type for the computer system is a timing attack [1], therefore development of the methods of counteraction to modern side channel attacks due to unauthorized information leakage is a relevant task.

2 RSA is a Modern System of Information Security

When developing a stable computer information security systems it is essential to provide restriction of the system functioning to bypass the subsystems protection and access delimitation. Cryptosystems based on elliptic curves have a high level of information security, but in practice, they are not widely used because of the implementation complexity [13].

The system of asymmetric cryptography allows realizing robust authentication of the parties, applying and verifying of digital signature, issuance and verification of public key certificates [9].

A security policy system should determine that authorised authority should issue a certificate of the public key only in the case that the key is given to an organization or an authorised person who will use this key. Thus specific organizational requirement should be developed.

Modern cryptosystem standard RSA algorithms usually use (name of the system is formed from the first letters of inventors' names—R. Rivest, A. Shamir, L. Adleman) with a key length of 1024 bits [8].

The RSA system that was first introduced in 1977 is perhaps the most popular system of protection of information with the public key.

The main operation that affects the stability and performance of asymmetric cryptosystems is modular exponentiation. The choice of modular exponentiation method that is resistant to time analysis and ensures advanced system performance is a priority task.

A lot of public-key cryptosystems use the function of discrete exponentiation [9]

$$f(n) = x^n (\mathrm{mod}\, m) \tag{1}$$

where

n is an integer number ($1 \le n \le m-1$),

m is a large number,

x is an integer number ($1 \le x \le m$).

To provide the sustainability of two-keys systems fairly large values of x and p must be used, therefore there is a need to use special methods to simplify and accelerate the calculation process of this function. Currently the most used methods are the following: binary method, β method, sliding window method, methods of fixed index, fixed basis methods and methods that use modules' special features [9].

A binary method uses binary image number $n = (n_{k-1} \ldots n_0)_2$. This method is performed in two directions. When reading "left to right" x^n is written as [9]:

$$x^n = x^{(n_{k-1} \ldots n_0)_2} = \left(\ldots \left(\left((x^{n_{k-1}})^2 x^{n_{k-2}} \right)^2 \ldots \right) x^{n_1} \right)^2 x^{n_0}. \tag{2}$$

In the binary method based on read "right to left" the following record is used [9]:

$$x^n = x^{(n_{k-1} \ldots n_0)_2} = \left(x^{2^0} \right)^{n_0} \left(x^{2^1} \right)^{n_1} \ldots \left(x^{2^{k-1}} \right)^{n_{k-1}} = \prod_{\{i | n_i = 1\}} x^{2^i}. \tag{3}$$

The B method is based on the image of exponent with the β base, that is $n = (n_{k-1} \ldots n_0)_\beta$. This method is also performed in two ways. When reading "left to right" [9]:

$$x^n = x^{(n_{k-1} \ldots n_0)_\beta} = \left(\ldots \left(\left((x^{n_{k-1}})^\beta x^{n_{k-2}} \right)^\beta \ldots \right) x^{n_1} \right)^\beta x^{n_0}. \tag{4}$$

When reading "right to left" [9]:

$$x^n = x^{(n_{k-1} \ldots n_0)_\beta} = \left(x^{\beta^0} \right)^{n_0} \left(x^{\beta^1} \right)^{n_1} \ldots \left(x^{\beta^{k-1}} \right)^{n_{k-1}} = \prod_{w=1}^{\beta-1} \left(\prod_{\{i | n_i = w\}} x^\beta \right)^w. \tag{5}$$

Sliding window method is based on an arbitrary partition into blocks (windows) of a binary image of exponent degree, that is $n = [w_{i-1}, \ldots, w_0]_2$. In this method, the windows should not have the same size.

In [9] two types of windows are considered: zero windows formed only by bit 0, and the odd window of at most w length, beginning and ending with bit 1.

When reading binary image of number n "left to right" [9]

$$x^n = \left(\left(\ldots \left(\left(x^{(w_{i-1})_2} \right)^{2^{|w_{i-2}|}} \cdot x^{(w_{i-2})_2} \right)^{2^{|w_{i-3}|}} \ldots \right)^{2^{|w_1|}} \cdot x^{(w_1)_2} \right)^{2^{|w_0|}} \cdot x^{(w_0)_2}. \quad (6)$$

When reading "right to left" [9]

$$x^n = \prod_{i=0}^{l-1} x^{(w_i)_2 \cdot 2^{l_i}} = \prod_{w \in \{1,3,\ldots,2^w-1\}} \left(\prod_{\{i|(w_i)_2 = w\}} x^{2^{l_i}} \right)^w, \quad (7)$$

where $l_i = \sum_{j=0}^{i-1} |w_j|$, for any $1 \le i \le l-1$, $l_0 = 0$.

The Laboratory of RSA Data Security offers the following measurements to improve the resistance to such type of attack [12]:

1. ensuring continuous execution time of all modular exponentiation, however in this case the productivity of defence system reduces;
2. entering additional delays to the algorithm, however if there are not enough added delays a violator still can perform the cryptanalysis using additional measurements;
3. masking, that is multiplying the ciphertext by a random number to the implementation of exponentiation. This method of counteracting to timing attack reduces the performance of information security system by 2–10 %.

Thus there is a need to develop a new approach of asymmetric cryptographic protection from timing analysis implementation without sacrificing performance.

3 Fuzzy Selection System of Modular Exponentiation Method

Latest researches have shown that the modern attacks on implementation, especially passive attack of time analysis, are the most dangerous type of attacker's illegal actions. Therefore, modern computer protection systems should provide robust resistance to time analysis, without reducing performance and memory cost.

As noted above, the main operation that affects the stability and performance of asymmetric cryptosystem is modular exponentiation. Choosing the method exponentiation by modulo, which resists time analysis and provides high system performance, is the priority task.

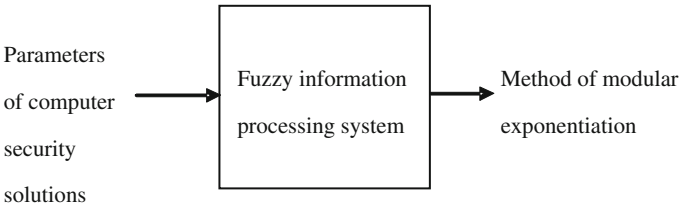

Fig. 2 General scheme of optimal selection of modular exponentiation method for distribution of computer system users' access

Considering the principle of Kochera [5], according to which the violator knows all about the encryption algorithm, except the key, as well as the actual implementation process of timing analysis that does not require the solving of the factorization problem, modular exponentiation exercise should be performed by means of individual method for each client.

In general the scheme of modular exponentiation choice method is shown in Fig. 2. In this case, the selection criteria are the basic parameters of the computer system of information protection, and the subsystem of the selection is the system of fuzzy information processing. The result of this system is one of the modular exponentiation methods that corresponds the input criteria of selection, using which computer system will ensure its optimum performance.

Since the distribution of users' access should consider the current system parameters such as performance, allowable memory consumption and the required level of timing analysis tolerance as well as fuzzy information about users, in order to solve this problem it is necessary to apply fuzzy logic [11].

For engineering problems Mamdani fuzzy mechanism is usually applied [11]. It uses a mini-max formulation of fuzzy sets. This mechanism includes the following steps [11]:

1. fuzzification procedure: degrees of truth are determined, that is the value of a membership function $MF_i(x)$ for the left part of each i rule (prerequisites);
2. fuzzy inference. Originally minimum "cut-off" level is defined for the left part of each of the rules $A_i = \min(MF_i(x))$, and then "truncated" membership functions of the conclusion $B_i = \min(A_i, B_i)$ are defined;
3. the composition or combining of received "truncated" function, where the maximum composition of fuzzy sets $MF(y) = \max(B_i(y))$ is used;
4. defuzzification or bringing to clarity. There are several methods of defuzzification, for instance, the method of the middle point or centroid method. The geometrical meaning of this value is the gravity canter for curve function according to the obtained exit.

Application of fuzzy logic in the creation of hardware and software means to implement the access distribution in the computer system will ensure cryptosystem resistance to time analysis in real time. Given access distribution is carried out by

selecting the optimal modular exponentiation method for each client and incorporating current parameters of CS.

The main criteria of a computer system working capacity are a high performance, optimal memory consumption and resistance to malicious attacks.

In order to perform the transmission of information computer system uses the network for user accessing. Such a data network can be divided into protected and unprotected parts (Fig. 3).

In an unprotected network users $K_1, K_2, \ldots, K_n$ can be random, for this reason they are not reliable in a server from a security point of view, thus there is a high probability of a user being a violator. In addition, this part of the network is usually not protected against failures due to environmental effects and is open for all types of contemporary attacks on implementation.

In a protected part of the network (see Fig. 3) users $K_{i1}, K_{i2}, \ldots, K_{im}$ are believed to be reliable and with regard to the security policy the existence of an internal violator is excluded. However, in this part of the network the possibility of passive timing analysis attack still remains [8, 13].

The server of a computer system consists of user identification subsystem, command subsystem and information processing unit (Fig. 4).

A user identification subsystem provides data to a processing unit about the required level of resistance to the timing analysis, including all the data about the user.

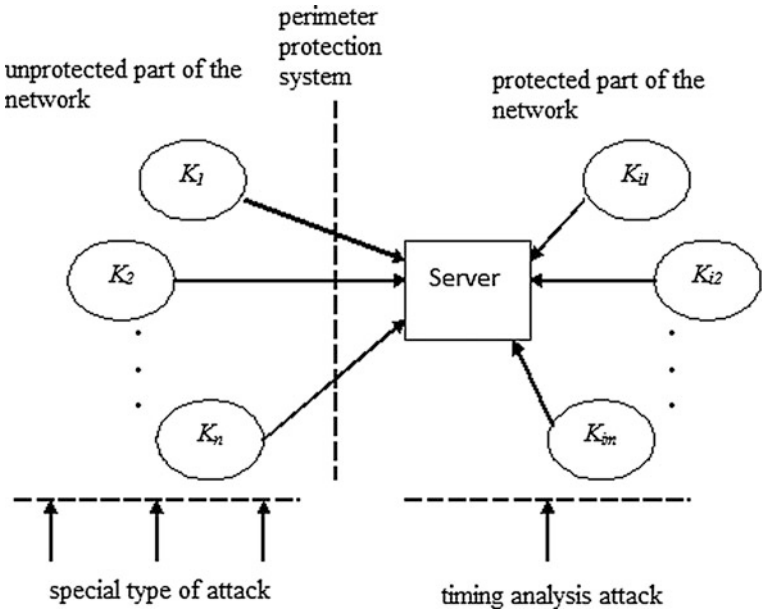

Fig. 3 The scheme of possible attacks on data transfer implementation in a computer system

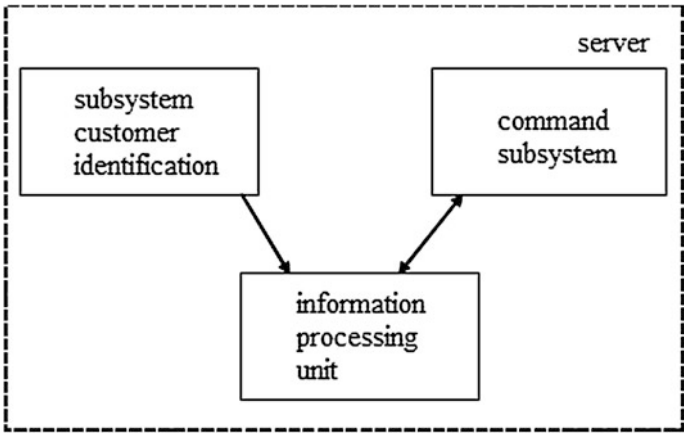

Fig. 4 The structure of a server of computer system

Users are known to a server by its IP-address and considering the "experience" of using the network they have their own level of reliability that can be set as the probability of failures in the transmission of information packets.

So, if a user is new to the system or has a very low level of reliability, the required level of resistance to timing analysis should be maximized. And vice versa for a user with a very high level of reliability the value of sustainability can go to 0, what will improve system performance.

Command subsystem of a server (see Fig. 4) provides a processing block with information about the computer system, namely the allowable memory consumption and the required level of performance.

In order to protect information in the network it is necessary to choose an optimal method of exponentiation by module to encrypt information or perform user authentication using cryptographic algorithm RSA. This problem is solved by an information processing unit, which is based on fuzzy logic, namely the mechanism of Mamdani fuzzy conclusion [11]. It handles input values of performance, memory consumption and resistance to timing analysis and provides an optimal method of modular exponentiation in each case to command subsystem which uses it to encrypt information. The main advantage of this unit is that it works in real time ensuring higher resistance of the system to malicious attacks as a violator will not know exactly the encryption algorithm [9, 12].

The general scheme of access distribution in a computer system is presented in Fig. 5.

A data processing block based on fuzzy logic is the basis of computer system protection. It is provided with selection criteria of modular exponentiation method, including the necessary level of resistance to the timing analysis R, productivity of cryptosystem P and the allowable memory consumption of the server M. Incoming fuzzy data are processed by a subsystem of optimal selection modular exponentiation method based on the mechanism of fuzzy conclusion according to Mamdani.

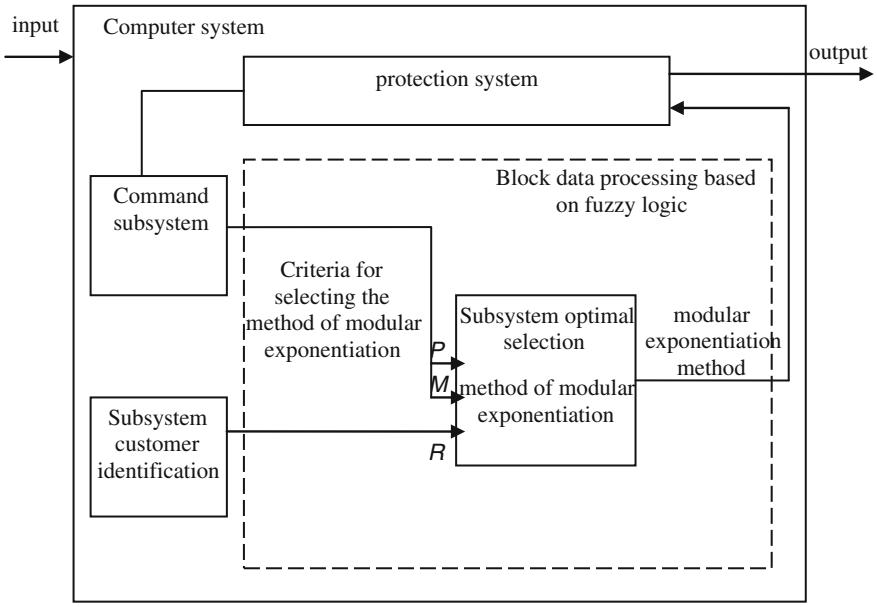

Fig. 5 General scheme of access distribution in a computer system based on fuzzy logic: *P* performance, *M* allowable memory expenses, *R* normalized resistance to timing analysis

The output of information by a processing block is a method of modular exponentiation that provides an optimal configuration of protection system regarding input selection criteria.

4 Conclusions

Thus, the structure of a computer network server introduced in the article helps to provide its optimal performance by means of access distribution to information resources. Further research of described fuzzy systems of the access distribution and its implementation on modern FPGA will allow us to realize a robust computer system against unauthorized access.

References

1. Bellezza, A.: Countermeasures against side-channel attacks for elliptic curve cryptosystems. In: Cryptology ePrint Archive, 2001/103 (2001). http://citeseer.ist.psu.edu/bellezza01countermeasures.html. Accessed 14 Sept 2014
2. Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Kaliski B.S. Jr. (ed.) CRYPTO'97, 17th Annual International Cryptology Conference on Advances in

Cryptology, Santa Barbara, CA, August 1997, pp. 513–525. Lecture Notes in Computer Science, No 1294. Springer, Heidelberg, (1997)
3. Convention on Cybercrime CETS No 185 The Cybercrime Convention Committee (T-CY), Strasbourg (2001). http://conventions.coe.int/Treaty/en/Treaties/html/185.htm. Accessed 14 Sept 2014
4. Corner, D.E., Stevens, D.L.: Internetworking with TCP/IP, Vol III: Client-Server Programming and Applications. Prentice Hall, Upper Saddle River, NJ (2000)
5. Gorbenko, I.D., Gorbenko, Y.I.: Prykladna kryptologia (Applied Cryptology). Fort, Kharkiv (2012)
6. Kshetri, N., Murugesan, S.: EU and US Cybersecurity strategies and their impact on businesses and consumers. Computer **10**(46), 84–88 (2013)
7. Kurose, J.F., Ross, K.W.: Computer Networking: A Top-Down Approach, 6th edn. Addison-Wesley, Boston (2011)
8. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer, Berlin (2007)
9. Moldovyan, A.A., Moldovyan, N.A., Sovyetov, B.A.: Kryptografiya (Cryptography). Lan', St Petersburg (2000)
10. Muir, J.: Techniques of Side Channel Cryptanalysis. Technical Report, Department of Combinatorics and Optimization, University of Waterloo (2001)
11. Shtovba, S.D.: Vvedeniye v teoriyu nyechotkikh mnozhestv i nyechotkuyu logiku (Introduction to the Theory of Fuzzy Sets and Fuzzy Logic). In: MATLAB. Exponenta (2001). http://matlab.exponenta.ru/fuzzylogic/book1/. Accessed 14 Sept 2014
12. Stallings, W.: Cryptography and Network Security: Principles and Practice, 6th edn. Prentice Hall, Upper Saddle River, NJ (2013)
13. Vasyltsov, I.V.: Ataky specialnoho vydu na kryptoprystroyi ta metody borot'by z nymy (The Attacks of Special Type on Crypto Devices and Methods of Dealing with Them). KOHPI, Kremenets (2009)