Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 108C (2017) 2100–2109

Procedia Computer Science

International Conference on Computational Science, ICCS 2017, 12-14 June 2017, Zurich, Switzerland

Identification of Quasi-Stationary Dynamic Objects with the Use of Derivative Disproportion Functions

Vyacheslav V. Kalashnikov[1,2,3*], Viktor V. Avramenko[2], Nikolay Yu. Slipushko[2], Nataliya I. Kalashnykova[4], and Anton E. Konoplyanchenko[2]

[1] *Tecnológico de Monterrey (ITESM), Campus Monterrey, Nuevo León, Mexico*
[2] *Sumy State University (SumDU), Sumy, Ukraine*
[3] *Central Economics and Mathematics Institute (CEMI), Moscow, Russian Federation*
[4] *Universidad Autónoma de Nuevo León (UANL), San Nicolás de los Garza, Nuevo León, Mexico*
kalash@itesm.mx, avr@sumdu.edu.ua, nkalash2009@gmail.com

Abstract

This paper presents an algorithm for designing a cryptographic system, in which the derivative disproportion functions (key functions) are used. This cryptographic system is used for an operative identification of a differential equation describing the movement of quasi-stationary objects. The symbols to be transmitted are encrypted by the sum of at least two of these functions combined with random coefficients. A new algorithm is proposed for decoding the received messages making use of important properties of the derivative disproportion functions. Numerical experiments are reported to demonstrate the algorithm's reliability and robustness.

Keywords: Identification of quasi-stationary dynamic objects, cryptographic systems, sums of key functions, identification algorithms

1 Introduction

In the modern Engineering Science and Technology, especially in the areas of Adaptive Control and Technical Diagnostics during a regular operation, the determination of a differential equation that describes a dynamic object is a very important and urgent task. Often there is an additional requirement of minimization of the time necessary for solving that task. Therefore, it is desirable to find the characteristics of the object at the current time without making use of any instantaneous values of the monitored processes. The coefficients of the differential equation can be changed due to some uncontrolled effects. In some cases, the order of the equation can also be changed. Even the type

[*] This research was partly financially supported from the SEP-CONACYT Grant CB-2013-01-221676.

10.1016/j.procs.2017.05.266

of the equation may be varied when a linear object becomes nonlinear. Finally, the parameters of the nonlinear elements are subject to variations as well.

A typical example of practical problems with the uncertainties of the above-mentioned kind is as follows. Consider a problem of technical diagnostics of a large class of quasi-stationary objects the static parameters of which (measured at a fixed time moment *t*) satisfy the following equation

$$y = k(t)x. \tag{*}$$

Here, x and y are the input and output parameters, respectively, and the (unknown) function $k(t)$ is assumed to vary much slower than the input function $x = x(t)$. If the considered technical device is damaged, the proportionality (*) is distorted and may follow the perturbed relationship

$$y = k(x,t)x + b(t), \tag{**}$$

where $b(t) \neq 0$.

The system of technical diagnostics should detect such deterioration and estimate its scale. The easiest way to do that would be comparing the values of functions (*) and (**) for the same values of x. However, since the ratio function $k(t)$ in (*) for quasi-stationary objects uses to change randomly its value with time, it becomes very difficult (if not impossible) to determine its value at a given time point.

Because of its importance, the challenging problem of identification of dynamic objects has been studied in many publications. Even though in the majority of works correlation methods, least squares techniques, and the Fourier series expansion of signals are usually employed, new algorithms for solving this problem appear regularly. For example, a structural parametric identification on the basis of the multi-frequency quantization is described in (Kartashev et al., 2015). The simulation method using correlative methods of identification is proposed in (Porkuyan and Kuznetsova, 2008). In (Medvedev, 2000), the algorithms of identification of parameters and of object order are discussed. All these methods are based on the recurrent observer derivatives. Some heuristic algorithms have also been studied (Pervushin, 2013).

However, all those methods require the observation of processes during a certain time interval, which is not always available. The main novelty of this paper is that we develop a new identification method making use of *only instantaneous* values of the input-output processes and their derivatives. This is done by exploiting the *derivative disproportion functions* (DDF) introduced previously in (Avramenko, 2000; Avramenko and Zabolotny, 2009; Avramenko and Karpenko, 2002) whereas their comprehensive description is found in (Kalashnikov et al., 2017).

The rest of the paper is arranged as follows. Section 2 states the problem, while Section 3 defines the derivative disproportion functions and lists dome of their important properties. The identification algorithm is described in Section 4. Section 5 deals with a numerical example and the results of numerical experiments. Section 6 presents the concluding remarks, while the acknowledgments and the list of references finish the paper.

2 Problem Statement

Consider a quasi-stationary dynamic object with one input and one output whose behavior is described by the differential equation

$$a_n y^{(n)} + a_{n-1} y^{(n-1)} + \ldots + a_0 F(y) = x(t), \tag{1}$$

where t denotes the time, $x(t)$ and $y(t)$ are the functions of input and output, respectively; and finally, F is a nonlinear operator (element) that affects (converts) the function $y(t)$. The main characteristics of the latter operator (element) as well as the upper bound of the order of equation (1) are assumed to be known.

In this paper, we restrict ourselves to the case, where both $x(t)$ and $y(t)$ are deterministic processes, although it isn't very difficult to examine more realistic noisy processes. The coefficients of equation (1) may be accepted as constants during the process of identification.

It is necessary to identify the coefficients of equation (1) by making use of *only instantaneous* values of input and output processes and their derivatives or to determine that there is a transient in the current time. (The proposed method doesn't identify the object during the transition process.) The task is completed by exploiting the *derivative disproportion functions* (DDF) introduced previously in (Avramenko, 2000; Avramenko and Zabolotny, 2009; Avramenko and Karpenko, 2002) and fully described in (Kalashnikov et al., 2017). For the paper to be self-sufficient, the definitions and key properties of these functions are presented in the following sections.

3 Derivative Disproportion Functions

In the competitive world of today, the value of information is constantly increasing and therefore, it is necessary to encrypt this information in order to hide it from an unauthorized use. The latter aim has led to the widespread use of cryptographic techniques within information systems, the most famous of which are Data Encryption Standard (DES, 1999), Advanced Encryption Standard (AES, 2001), and the Rivest-Shamir-Adleman (RSA) cryptosystem (Rivets et al., 1978). But the new powerful super-computers and the technologies of network and neural computing that have arisen since 2000, bring up the revision of the previous cryptographic systems that had been considered as absolutely reliable. Therefore, the development of new approaches to the creation of cryptosystems is relevant.

Almost all cryptosystems use integers as keys. The greater the key length is, the more difficult it is to "break" a cryptosystem by fitting a key or by solving a factorization problem. The transition from integers to real numbers, or even better to real type functions is expected to considerably complicate the task of cryptanalysis and to increase the stability of cryptosystems.

The new methods of classifying information can be developed on the basis of the use of disproportion functions. Disproportion functions on the derivatives and on the values were proposed and studied in (Avramenko, 2000; Avramenko and Zabolotny, 2009; Avramenko and Karpenko, 2002).

In this part of the paper, we recall the capability of such an approach for classifying and declassifying of both analog signal and the signal in the form of a sequence of symbols from the specified alphabet (Avramenko, 2000; Avramenko and Zabolotny, 2009). This cryptosystem is based on the use of disproportion functions. The input symbols are encoded by the sum of real functions (keys) combined with random coefficients. Due to the disproportion functions, there appeared an opportunity to recognize the sum of which functions is included in the received signal at the current moment, despite the unknown coefficients involved, and thus to recognize the encrypted symbols.

Derivative disproportion functions characterize numerical functions. They permit to obtain a quantitative assessment of deviation of a numerical function from the power function $y = k \cdot x^n$ for a given value of the argument, regardless of the multiplier *k*. Here $n \geq 1$ is an integer.

The *n*-th order derivative disproportion of the function $y = y(x)$ with respect to x ($x \neq 0$) is defined as follows:

$$@d_x^{(n)} y = \frac{y}{x^n} - \frac{1}{n!} \cdot \frac{d^n y}{dx^n}. \tag{2}$$

In the particular case of $n = 1$ (order 1), formula (2) of the derivative disproportion is reduced to

$$@d_x^{(1)}y = \frac{y}{x} - \frac{dy}{dx}. \tag{3}$$

As it could be expected, for the linear function $y = kx$ its disproportion of order 1 is zero for any value of the coefficient *k*. The symbol @ is chosen to designate the operation of determination of disproportion. The symbol "*d*" is selected to refer to the function's derivative as the main object of disproportion calculated. Finally, the left-hand side of (3) is read "a*t d one y with respect to x*".

If a function is specified in the parametric form, the *n*-th order derivative disproportion (2) is determined by applying the rules of calculation of $\frac{d^n y}{dx^n}$ under the parametric dependence of *y* upon *x*. In particular, the first-order derivative disproportion of the function defined parametrically as $x = \psi(t)$ and $x = \varphi(t)$ (where *t* is the parameter, and $\varphi(t) \neq 0, \varphi'(t) \neq 0$) has the form

$$@d_x^{(1)}y = @d_{\varphi(t)}^{(1)}\psi(t) = \frac{y}{x} - \frac{y'_t}{x'_t} = \frac{\psi(t)}{\varphi(t)} - \frac{\psi'(t)}{\varphi'(t)}. \tag{4}$$

Clearly if $\psi(t) = k\varphi(t)$ for some constant *k*, its derivative disproportion (4) equals zero in all the area in which the functions $y = \psi(t)$ and $x = \varphi(t)$ are simultaneously defined.

Lemma 1 [7]. *Every derivative disproportion function of order n boasts the following properties:*

1. *Multiplying the function y by any scalar k leads to scaling its derivative disproportion by the same scalar.*
2. *The order n derivative disproportion of a sum (difference) of functions equals to the sum (difference) of their derivative disproportion.*
3. *For the linear function $y = kx$, its derivative disproportion of order 1 is zero for any value of the coefficient k.*

Proof. It is readily verified by simple algebraic manipulations with the use of definition (2). ■

Remark 1. In other words, the operator $@d_x^{(n)}$ defined on the space $C^n(\Omega)$ of *n* times smoothly differentiable real functions is linear over this space. ■

4 Identification Algorithm

Let us rewrite equation (1) in the form of the sum of key functions with unknown coefficients:

$$f_0(t) = \sum_{i=1}^{n} k_i f_i(t), \tag{5}$$

where by the function f_0 we denote the input process *x*, while the functions $f_i = f_i(t), i = 1, 2, \ldots, n,$ represent the output process $y(t)$ and its derivatives. The identification problem applied to quasi-stationary dynamic objects can be illustrated with the following example.

Example 1. Consider a communication system transmitting symbols (signals) encoded with a cryptosystem $\mathcal{K}$ based on key functions $f_i = f_i(t)$, each defined on a (time) interval $t \in [0, T_i], T_i > 0, i = 1, \ldots, m$. The functions are assumed smooth and *n* times differentiable. A symbol transmitted at the time moment *t* is encoded by the sum of (at least two) key functions with possible time delays (shifts) $\tau_i \in [0, T_i], i = 1, \ldots, m.$ For example if the transmitted symbol is encoded as the sum of two key functions f_p and $f_q, 1 \le p, q \le m,$ the signal transmitted to the communication channel has been encoded as

$$y(t) = k_p f_p\left(t + \tau_p\right) + k_q f_q\left(t + \tau_q\right), k_p > 0, k_q > 0. \tag{6}$$

It is assumed that the invader (hacker) who may have got an unauthorized access to the channel is informed of neither the key functions f_i nor their time delays (shifts) τ_i , nor the coefficients $k_i,\ i = p, q.$

At the receiver end of the communication system, the full list of key functions and their delays is known but which of them (and with what coefficients) are involved in the received signal (6) is to be detected. The recognition of these functions and their coefficients in (6) permits to decode the current symbol $y(t)$.

The problem of detecting both the key functions and their coefficients in (6) is solved by the algorithm proposed in the next subsection.

4.1 Algorithm's Description

The problem in question is hard to solve since the key functions and their coefficients can be detected only approximately. The received message $y(t)$ is expanded in time, so exact or approximate derivatives of this function are needed. When the data are discrete, e.g., $\left\{y\left(t_j\right)\right\}_{j=0}^{N-1}$, then the desired approximate "derivative" of the (discretized) function $y(t)$ is found by a special method, similar to that by Gregory-Newton (*cf.*, Khan et al., 2003).

The algorithm is quite complicated, and due to the space restriction, here we present its description for $m = 3$ only (the complete version can be found in (Kalashnikov et al., 2017) and other publications of the authors).

The main idea of the general algorithm is as follows: if the key function delays (shifts) $\tau_i, i = 1\ldots, m$, are known, we may represent the received message $y(t)$ as the sum of all key functions with yet unknown coefficients k_i (for simplicity, assume that all delays are zero):

$$f_0(t) = \sum_{i=1}^{m} k_i f_i(t)\,. \tag{7}$$

Then we have to calculate their coefficients at the current moment *t*. Coefficients will be equal to zero for those functions that are not involved in the encrypted signal (7).

As we mentioned above, the description of the algorithm will be given for the case $m = 3$ only. The algorithm consists of m steps (that is, 3 in our case).

Step 1. Select arbitrarily one of the key functions, for instance, the first one $f_1 = f_1(t)$. By making use of (3) calculate the derivative disproportion for the signal $f_0(t)$ and denote it as $F_{01}(t) := @d_{f_1}^{(1)} f_0(t)$. Besides, derivative disproportions $F_{21}(t)$ and $F_{31}(t)$ are calculated for the key functions $f_2(t)$ and $f_3(t)$ with respect to $f_1(t)$. Due to the linearity of operator @ (*see*, Remark 1), formula (7) yields for $m = 3$:

$$
\begin{aligned}
F_{01}(t) &\equiv @d_{f_1}^{(1)} f_0(t) = \frac{f_0(t)}{f_1(t)} - \frac{f_0{}'(t)}{f'_1(t)} = k_1 \cdot 0 + k_2 \left[\frac{f_2(t)}{f_1(t)} - \frac{f'_2(t)}{f'_1(t)} \right] + \\
&+ k_3 \left[\frac{f_3(t)}{f_1(t)} - \frac{f'_3(t)}{f'_1(t)} \right] = k_2 @d_{f_1}^{(1)} f_2(t) + k_3 @d_{f_1}^{(1)} f_3(t) \equiv k_2 F_{21}(t) + k_3 F_{31}(t).
\end{aligned}
\tag{8}
$$

Here, the first term on the right-hand side of the upper line of (8) is zero due to assertion 3 of Lemma 1.

Step 2. Again, pick up randomly one of the remaining derivative disproportions $F_{21}(t)$ and $F_{31}(t)$; let it be, for instance, $F_{21}(t)$. Now we compute the derivative disproportions of the functions $F_{01}(t)$ and $F_{31}(t)$ with respect to $F_{21}(t)$; denote them as $F_{0121}(t)$ and $F_{3121}(t)$, respectively.

Applying the operator of the derivative disproportion of order 1 to both sides of (8), making use of its linearity and property 3 of Lemma 1 one easily gets

$$
F_{0121}(t) \equiv \frac{F_{01}(t)}{F_{21}(t)} - \frac{F'_{01}(t)}{F'_{21}(t)} = k_2 \cdot 0 + k_3 \left[\frac{F_{31}(t)}{F_{21}(t)} - \frac{F'_{31}(t)}{F'_{21}(t)} \right] \equiv k_3 F_{3121}(t).
\tag{9}
$$

Step 3. Relationship (9) shows the linear dependence of the function F_{0121} on the function F_{3121}. Therefore, based on property 3 of Lemma 1, we conclude that the derivative disproportion function $F_{01213121}(t)$ of the function F_{0121} with respect to F_{3121} is zero for all feasible t:

$$
F_{01213121}(t) \equiv @d_{F_{3121}}^{(1)} F_{0121}(t) = \frac{F_{0121}(t)}{F_{3121}(t)} - \frac{F'_{0121}(t)}{F'_{3121}(t)} = k_3 - k_3 = 0.
\tag{10}
$$

Now one can use relations (8) and (9) in the reverse order and calculate the desired values of the unknown coefficients k_i. Indeed, first from (9) one readily gets

$$
k_3 = \frac{F_{0121}}{F_{3121}};
\tag{11}
$$

the latter, in its turn, together with (8) implies:

$$
k_2 = \frac{F_{01} - k_3 F_{31}}{F_{21}}.
\tag{12}
$$

Finally, by substituting the just found k_2 and k_3 in (7), one deduces the value of k_1 :

$$
k_1 = \frac{y(t) - k_2 f_2(t + \tau_2) - k_3 f_3(t + \tau_3)}{f_1(t + \tau_1)}.
\tag{13}
$$

The algorithm stops having decoded the received message (quasi-stationary dynamic object) $f_0(t)$ by having detected the unknown coefficients associated with the involved key functions. All coefficients related to the non-used key functions are zero. The object has been identified. ■

Remark 2. If the disproportion (10) isn't equal to zero, it is necessary to check the following points:

1 There may be a transient process in the object. When this process is finished, the disproportion will be equal to zero.

2 A non-linearity has appeared in the object, or the parameters of the nonlinear element have been changed.

3 The order of the equation is greater than it was previously estimated. ■

This algorithm can be used for rapid identification of quasi-stationary dynamic objects if the input and output processes are smooth. No interferences are allowed.

Remark 3. As it can be easily concluded, the knowing of the list of involved functions and their delay (shift) values τ_i is indispensable for the implementation of this simplified version of the decoding algorithm. The more sophisticated procedures that may be needed to decipher the received message in the lack of such important information are described in (Avramenko, 2000; Avramenko and Zabolotny, 2009).

5 Numerical Illustration

The efficiency of the developed algorithm was tested by using computer simulations. Namely, consider the Duffing equation that is employed for describing many kinds of nonlinear objects:

$$\frac{d^2x}{dt^2} + 2\alpha\frac{dx}{dt} + \omega_0^2 x + hx^3 = G\cos\left(\omega_1 t + \theta\right), \tag{14}$$

where *t* is the time variable, *x* (*t*) is a system's deviation from the initial state, α is a dissipation factor (damping), ω_0 and *h* are the coefficients depending on the system parameters, and finally, G, ω_1, θ are the amplitude, frequency, and phase of the external influence.

Before modeling, the values of coefficients and parameters of external influence were specified randomly in equation (14). Then the Cauchy problem was solved by the use of Runge-Kutta method of the 4th order with the step time equal to 0.01s. The processes *x*(*t*) and *dx*/*dt* were thus numerically obtained. The second derivative d^2x/dt^2 was calculated with the aid of the Newton-Stirling numerical method using the first derivative.

The coefficients of the differential equation that were first defined and that calculated are shown in Table 1.

t	DDF	k_1		k_2		k_3		k_4	
		Def.	Calc.	Def.	Calc.	Def.	Calc.	Def.	Calc.
0.3	$-1.68\cdot10^{-7}$	0.13	0.1300	0.062	0.06233	3.02	3.02	1	1.00003
1.42	– 0.0002	0.13	0.1301	0.062	0.06098	73.1	72.45	1	1.00322

Table 1: Coefficients (defined and calculated) of the differential equation

The minor deviations are associated with the choice of the time quantization step for modeling and calculation of derivatives.

Figure 1 shows a plot of the derivative disproportion function (DDF) (10) if the parameter 2α changed abruptly from 0.23 to 0.35 when the time is equal to 0.57 seconds. As a result, the DDF (10) has stopped being zero.

At the end of the transition process, the values of DDF (11) are again equal to zero, and the coefficient k_3=0.35 is constant.

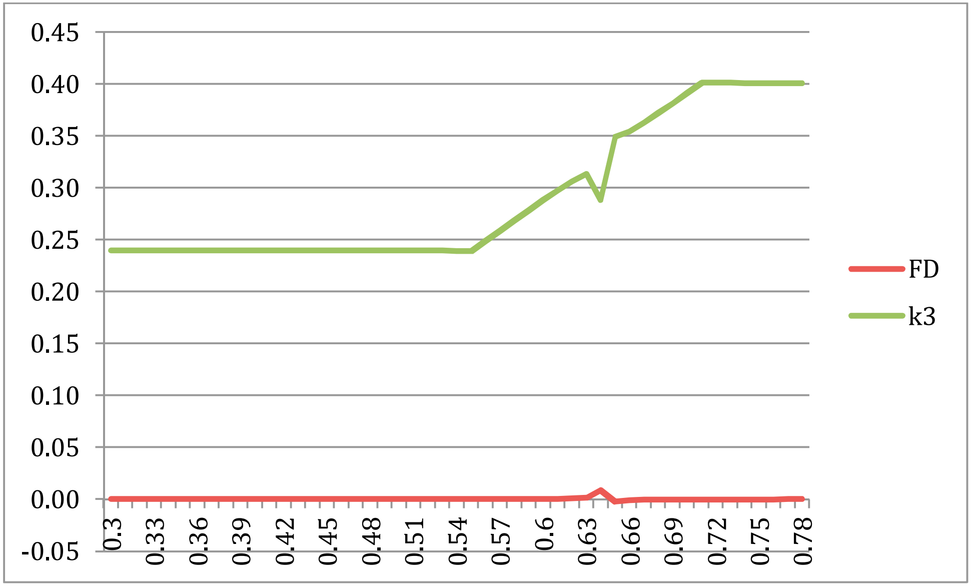

Figure 1: An irregularity occurs at t = 0.57

Figure 2 depicts the change of the ratio k_3 from 0.23 to 0.38 in the time interval 0.57 to 0.72. On this interval, the DDF (10) wasn't zero, so it is impossible to calculate the coefficients of equation (7). However, at the end of the transition process, the DDF (10) again becomes zero, and the coefficient k_3 received the constant value of 0.38.

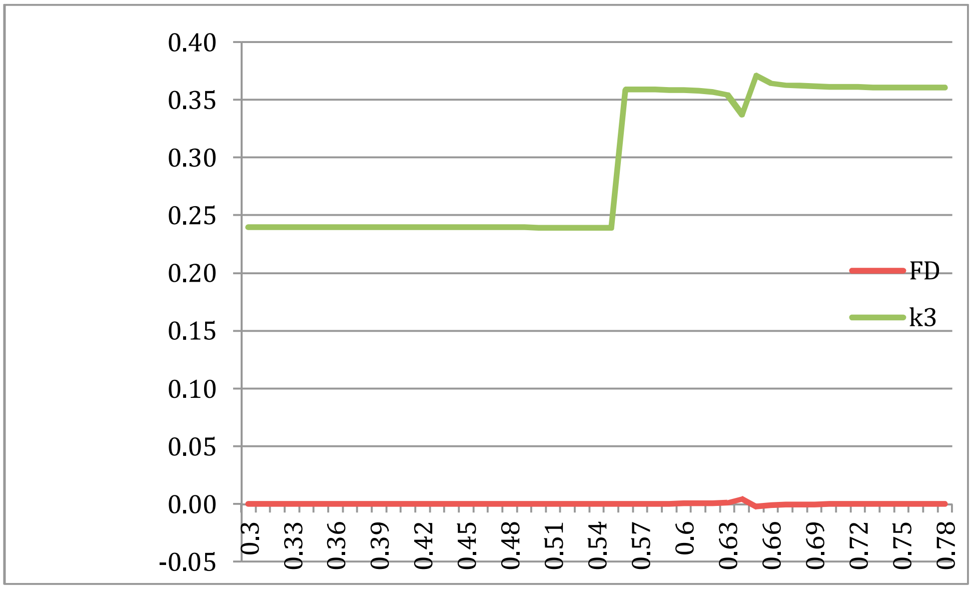

Figure 2: Another irregularity happens in the time interval 0.57 to 0.72

These minor fluctuations of the values of k_3 are the result of numerical differentiation with the use 6-order differences.

Those examples demonstrate the proposed algorithm's performance. According to the rapidly detected fluctuations and their derivatives, the algorithm is robust and allows one to implement efficiently the operational control of the parameters of dynamic systems.

6 Concluding Remarks

The determination of a differential equation that describes a dynamic object is a very important and challenging task. An additional requirement of minimization of the time necessary for solving that task is quite frequent.

A plenty of various numerical algorithms has been developed to solve the identification problem. However, all those methods require the observation of processes during a certain time interval, which is not always possible. The main novelty of this paper is in that we propose a new identification method making use of *only instantaneous* values of the input-output processes and their derivatives. The task is completed by exploiting the *derivative disproportion functions* (DDF) introduced previously in (Avramenko, 2000; Avramenko and Zabolotny, 2009; Avramenko and Karpenko, 2002) and comprehensively described in (Kalashnikov et al., 2017).

Namely, we propose a cryptosystem where real functions are used as keys. The example is provided to illustrate the operation of such a system where symbols are encoded by the sum of the key functions with random coefficients. Decryption occurs with the help of the first order derivative disproportion functions calculated for the received signal and the key functions.

For a practical application of such cryptosystems, one should bear in mind that in the process of calculation of the coefficients during decoding, there may arise examples of division by small numbers, or a ratio of two numbers both close to zero. This can lead to information distortion. Therefore, the encrypted message must be decoded before it is transmitted to a communication channel. If necessary, the message must be encrypted once again with other coefficients in the hope that the generator of random numbers varies the obtained coefficients of the key functions.

Acknowledgments

This research was partially supported by the School of Engineering and Science (EIC) of the Tecnológico de Monterrey (ITESM), Campus Monterrey, and the Research Grant No. CB-2013-01-221676 from SEP-CONACYT (Mexico).

The authors would also like to express their profound gratitude to the three anonymous referees whose valuable comments and suggestions has helped a lot improve the presentation.

References

Kartashev, V.Ya., Kartasheva, L.V., and Samoilenko, S.S. (2015). *Structural and parametric identification of dynamic objects in real time.* Transactions of Kemerovo State University (Vestnik

Kemerovskogo Gosudarstvennogo Universiteta), **1**(1): 13–18 (*in Russian*). http://cyberleninka.ru/journal/n/vestnik-kemerovskogo-gosudarstvennogo-universiteta

Porkuyan, O.V., and Kuznetsova, E.V. (2008). *Identification of dynamic objects of various structures on the base of Hammerstein parallel models*. East European Journal of Advanced Technologies (Vostochnevropeiskiy Zhurnal Peredovykh Tekhnologiy), **4**(1): 47–50 (*in Russian*). http://elibrary.ru/download/elibrary_23128219_41663644.pdf

Medvedev, M.Yu. (2000). *Identification of dynamic objects by evaluating the derivatives of the observed signals*. Proceedings of South Ural University (Izvestiya Yuzhnouralskogo Universiteta), **15**(1): 1 (*in Russian*). http://cyberleninka.ru/article/n/identifikatsiya-dinamicheskih-obektov-po-otsenkam-proizvodnyh-nablyudaemyh-signalov#ixzz40tqRhEoU

Pervushin, V.F. (2013). *On a nonparametric model of linear dynamic objects*. Transactions of Tomsk State University (Vestnik Tomskogo Gosudartvennogo Universiteta)*,* **25**(4): 95–104 (*in Russian*) http://cyberleninka.ru/article/n/o-neparametricheskoy-identifikatsii-lineynyh-dinamicheskih-obektov#ixzz40umcKUrT

Avramenko, V.V. (2000). The measures of non-proportionality of real functions as applied to solving diagnosis problems. Transactions of Sumy State University (Visnyk Sumskogo Derzhavnoho Universitetu, SumDU), 2000, **16**(1): 12–10120 (*in Russian*).

Avramenko, V.V., and Zabolotny, M.I. (2009). *A Way of Data Coding*. Patent UA H04L 9/00 №42957, Ukraine.

Avramenko, V.V., and Karpenko, A.P. (2002). *Recognition of fragments of given standards in an analyzed signal with the aid of disproportionality functions*. Transactions of Sumy State University (Visnyk Sumskogo Derzhavnoho Universitetu, SumDU), 2002, **34**(1): 96–101 (*in Russian*).

Kalashnikov, V.V., Avramenko, V.V., Kalashnykova, N.I., and Kalashnikov-Jr., V.V. (2017). *A cryptosystem based upon sums of key functions*, to appear in the International Journal of Combinatorial Optimization Problems and Informatics, 11 p. ISSN 2007-1558.

U.S. Department of Commerce/National Institute of Standards and Technology Data Encryption Standard (DES) Federal Information (1999). Processing Standards Publication 46-3, October 25; http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

Federal Information Processing Standards Publication 197 November 26, 2001, Specification for the ADVANCED ENCRYPTION STANDARD (AES) http://csrc.nist.gov/publications/fips/fips197/fips197.pdf

Rivest, R., Shamir, A., and Adleman, L. (1978). *A method for obtaining digital signatures and public – key cryptosystems*. Communications of the ACM, **21**(2): 120–126. doi: 10.1145/359340.359342

Khan, I.R., Ohba, R., and Hozumi, N. (2003). *Mathematical proof of closed form expressions for finite difference approximations based on Taylor series*. Journal of Computational and Applied Mathematics, **150**(3): 303–309.