NONLINEAR-DYNAMIC SYSTEMS OF CONFIDENTIAL COMMUNICATION: CLASSIFICATION, SIMULATION, EXPERIMENT

Igor Izmailov
Dept. of Quantum Electronics & Photonics,
Tomsk State University,
Russia
izmi@elefot.tsu.ru

Il'ia Romanov
Dept. of Quantum Electronics & Photonics,
Tomsk State University,
Russia
izmi@elefot.tsu.ru

Boris Poizner
Dept. of Quantum Electronics & Photonics,
Tomsk State University,
Russia
pznr@elefot.tsu.ru

Denis Shergin
Dept. of Quantum Electronics & Photonics,
Tomsk State University,
Russia
pznr@elefot.tsu.ru

Abstract

A classification and a number of new confidential communication systems are introduced on the basis of chaos (or noise) generators. Heuristic nature of the classification lets to perform meaningful development of nonlinear-dynamic cryptosystems. Mathematical model and its features are considered, as well as experimental implementation of deterministic chaos generator for a variant of such cryptosystem. It's based on a radioelectronic circuit, which contains a nonlinear element, a photodiode, and a length of fiber-optics line, which is responsible for time lag in the feedback loop.

Key words

Applications, Chaos, Nonlinear systems, Hybrid systems, Modeling, Synchronization.

1 Introduction

The system engineering of confidential communication is actual always, while there is a need for protection of a privacy of correspondence. Today new impulse to development of messages protection technologies is given by the theory of deterministic chaos. Usage of devices with chaotic dynamics (generators of deterministic "noise") as a basis of steganography systems is reasonable since such systems imply mixing of a message with noise, thus concealing the fact of the message transmission. But this (steganographic according to the definition) method of confidential communication is traditionally used with noise-like signals, which have a well-developed theory and a long history. Against that background a cryptological application of radiophysical and optical systems with a complex dynamics seems to be less traditional and capabilities of such systems aren't evident, because in that case it's assumed that internal structure of the cryptosystem is known and channels of communication and synchronization are available for everyone [Vladimirov, Izmailov, Poizner. 2008]. Thus a key (i.e. a parameters values set of the device – in our case) is transmitted by means of the opened or closed communication channel, in depending on a type of the system of confidential communication, as the cryptograpny paradigm provides. Similar ideas can be found in the review by A.S. Dmitriev [Dmitriev, Starkov, 1998, p. 26] in terms of "masking tasks" and "confidentiality tasks".

Nonlinear-dynamic cryptosystems can be brought into a line with classical ones, if one can prove that: a) there is no polynomial algorithm of encryption algorithm's inversion without knowledge of encipherer's parameters; b) having a message and an encrypted message the key can be found with exponential complexity. Therefore there is a problem of finding for nonlinear-dynamic cryptosystems some correct analogues of the known definitions: polynomial and exponential algorithm complexity. Having this nontrivial task completed one can:

a) unify principles and methods of cryptostrength estimation for ciphers, which are described by a system of differential equations or a discrete map, and may be traditional ciphers;

b) develop methods of ciphers' generation with given strength.

Table 1. Extension of cryptosystems' classification by location of a chaos generator, decipherer's working mode, number of channels and their functions

Decipherer's working mode	Purpose of a chaos generator (position to the system)		
	Parameters of a chaos (noise) generator aren't a key (SIG is outside the system)	Parameters of a chaos generator are a key (χG is inside the system)	Parameters of an internal χG are a key, an external χG (NG) is a SIG, χIG or (S+χ)IG
Dual-channel with a dedicated synchronization line (Fig. 1 and 2)			
Chaotic response	Fig. 1, *a*	Fig. 1, *b*	Fig. 1, *c*
Active synchronization	—	Fig. 2	Fig. 2
Dual-channel without a dedicated synchronization line (Fig. 3)			
Chaotic response	—	Fig. 3, *a*	—
Active synchronization	—	Fig. 3, *b*	—
m-channel (of *m*, M_1, M_2 type) with *n/m* number of pure synchronization lines (Fig. 4)			
Chaotic response	+, $n \neq 0$	Fig. 4, *a*	+, $n \neq 0$
Active synchronization	—	Fig. 4, *b*	+, $n \neq 0$

First purpose of the paper is composition of essential classification of nonlinear-dynamic confidential communication systems, which contains not only well-known devices, but proposed ones by authors, as well. Second purpose is a detailed analysis of a model and a prototype device of developed deterministic chaos generator. The generator is built on radioelectronics and fiber-optics elements and is a base of the encipherer in its turn of one of the proposed nonlinear-dynamic confidential communication systems.

2 Classification of nonlinear-dynamic cryptography systems and possible ways of its evolution

Complexity of data security facilities' development [Dmitriev, Panas, 2002] in combination with the variety of their applications leads to a diversification of proposed methods and constructions of nonlinear-dynamic cryptography. So, the situation requires a classification of such methods and constructions. Expanding a [Vladimirov, Negrul, 2000] classification authors propose Table 1, which is illustrated by Fig. 1-5.

In order to unify descriptions of structure features of the discussed cryptosystems let's introduce the following acronyms: DL – data line, SL – synchronization line, SDL – synchronization and data line, χIG – chaotizating impact generator (χG – chaos generator or NG – noise generator), SIG – synchronizing impact generator, i.e. synchronizer (χG or NG or regular signals generator), (S+χ)IG – synchronizing and chaotizating impact generator (χG or NG), FT – functional transformer of signals without internal feedback loop (elementary FT), D – data signal, apostrophe sign (′) attributes decipherer, a FT_i' transformer is considered to be nominally identical to a corresponding FT_i of a cipherer. This condition is achieved by identity of appropriate parameters values of FT_i and FT_i'. Just this parameters values set is the key of the given system of nonlinear-dynamic cryptography.

Fig. 1 depicts schematic layout of dual-channel systems with a dedicated synchronization line. Fig. 1, *c* differs by presence of both external χIG and internal χG. It's obviously functional, its advantages and disadvantages require further discussion. For example, "underexcited" mode of internal dynamic system (based on FT_1 and FT_2) seems to be interesting. A cryptography key for the system is a set of FT_1 or FT_2 parameters.

Structure of dual-channel systems with a dedicated line of active synchronization is depicted on Fig. 2. Transmitter and receiver equitable influence each other, producing mutual synchronization in such systems. In the case of forced synchronization the receiver produces a unidirectional impact. The concept of "coordinating" synchronization consists in synchronization of the transmitter and the receiver between each other by an external independent signal. Since coordinating synchronization doesn't imply absence of mutual or forced one, there are 2 possible variants of combined synchronization, which is depicted on Fig. 2. It's necessary to emphasize that if there is a forced synchronization line or coordinating forced synchronization line, then FT_1' will unavoidably differ from FT_1 due to asymmetry of the cryptosystem's χG interaction.

Apparently it's impossible to build a cryptosystem with a dedicated channel of active synchronization, which contains only external χG (NG) – see Table 1. It's so because according to definition of active synchronization a decipherer must contain a chaos generator, whose parameters are a key, therefore a cipherer must contain that component also.

The idea of dual-channel systems without a dedicated synchronization channel consists in usage of a signal transmitting over a data line of a cryptosystem

for synchronization of another system. Thereby the data line and synchronization line become synchronization and data line, functional transformers and / or chaos generator of the cipherer become looped with

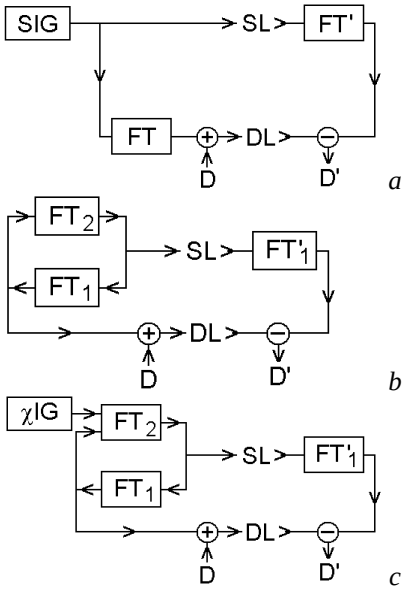

Figure. 1. Schematic layout of dual-channel systems of nonlinear-dynamic cryptography with a dedicated synchronization line and deciphering in the chaotic response mode: with external SIG (*a*), with internal χG (*b*), internal χG and external χIG (c). *a* and *b* schemes are equivalent to the ones described in [Vladimirov, Negrul, 2000] and [Kal'yanov, Grigor'yants, 2001].

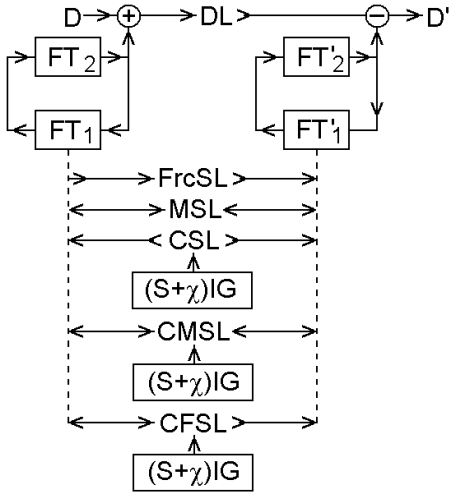

Figure. 2. Schematic layout of dual-channel systems of nonlinear-dynamic cryptography with a dedicated synchronization line and an internal χG. Main types of active synchronization are depicted: mutual (MSL), forced (FrcSL), coordinating (CSL); and mixed: mutual coordinating (CMSL) and forced coordinating (CFSL).

common feedback loop, thus they are not independent anymore, by creating a united dynamical system. Structures of the systems, which use chaos parameters as a key (χG is inside the system), and decipherer uses both chaotic response and coordinating active synchronization, are depicted on Fig. 3. A cryptosystem on the basis of nonlinear ring interferometer (NRI) with rotation of optical field in the feedback loop at 180° [Izmailov, Poizner, 2001] operates according to the principle illustrated by Fig. 3, *a*.

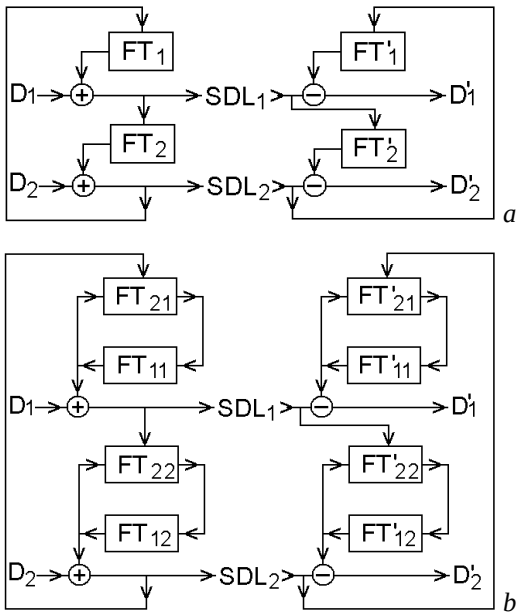

Figure. 3. Schematic layout of dual-channel systems of nonlinear-dynamic cryptography without a dedicated synchronization line and with an internal χG. Decipherer uses chaotic response (*a*) or coordinating active synchronization (*b*).

It seems that one can use not only coordinating active synchronization in a cryptosystem, but some types of mixed synchronization also. Due to incompatibility of presence of external χG with absence of a dedicated synchronization line it's impossible to implement a cryptosystem without a dedicated synchronization line with external χG (NG) – see Table 1.

Using the described above method of cryptosystems' synthesis, it's possible to create *m*-channel systems without a dedicated SL and with internal χG – see Fig. 4. Replacing any of the input data lines D_i with a signal of external χG_i (or NG_i) leads to switching a corresponding SDL_i to a coordinating line (CL_i). Therefore one can get a system with non-zero portion of coordinating lines. In that case the external χG (NG) acts as (S+χ)IG.

If one breaks feedback loop in the cipherer of a system with chaotic response (Fig. 4, *a*) by deleting FT_{i-1}, then it will be a cryptosystem without internal χG, which has an external SIG. The cryptosystem based on NRI with field rotation at $\Delta=\pi M/m$ angle works according to the principle, which is illustrated by Fig. 4, *a*.

It's easy to see that any individual FT_{ij} (on Fig. 4, *a)* or an internal χG_{ij} consisting of FT_{1ij} and FT_{2ij} (on Fig. 4, *b*) connects output of *i* adder unit with input of *j* adder unit. It's obvious that number of such χG_{ij} and FT_{ij} can vary from *m*-1 to m^2, while they can form

(non-)closed or combined complex configuration of interconnections (linear or diverging/converging star or ring and so on), which, in its turn, can be a key. For instance, for two-circuit NRI [Izmailov, Lyachin, Poizner, 2007] with 180° and 120° angles of rotations in feedback loops the scheme is depicted on Fig. 5. Capability of cryptostrength increase is actual most for the systems, in which large values of m can be achieved e.g. for spatial distributed devices.

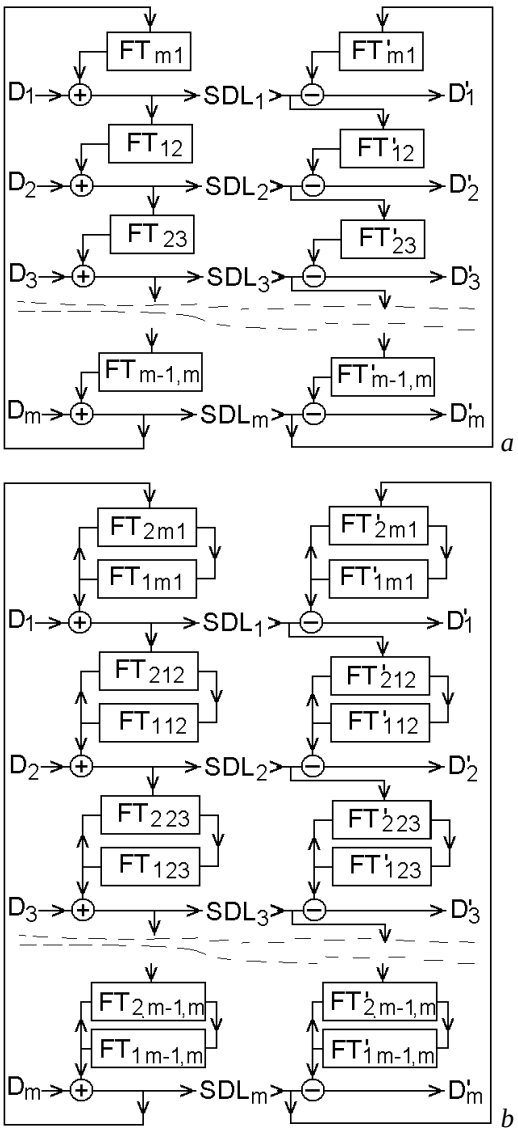

Figure. 4. Schematic layout of m-channel systems of nonlinear-dynamic cryptography without a dedicated synchronization line and with an internal χG. Decipherer uses chaotic response (*a*) or coordinating active synchronization (*b*).

Fig. 4, *a* is equivalent to Fig. 4, *b*, if one replaces elementary FT with χG, which consists of two FTs. Therefore it's rightful to say that a system with active synchronization is a system with chaotic response of chaos generators. Examination of universality of the feature is a separate research issue.

It's necessary to emphasize that in the case of m-channel cryptosystems a cipherer can be interpreted as single united dynamical system with l dynamic variables (where $l \gtrless m$). So the cryptosystem can be treated as single-channel one, but with l-dimensional data line (meaning that there is a simultaneous transmission of l signals).

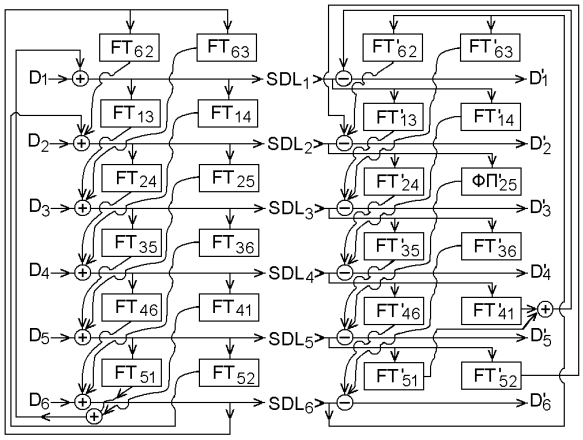

Figure. 5. Schematic layout of a cryptosystem, which corresponds to two-circuit NRI in the case of 180° and 120° angles of rotations in feedback loops.

It was supposed above that external χG or NG (i.e. its parameters or the signal itself) are not a key. But there can be a situation when transmitting and receiving sides get (independently from each other) a signal from a previously selected common χG (NG) and according to a previously selected principle. In that case the unknown to 3rd party χG (NG) and the principle (or its changing part) is the key. It seems that the proposed approach is promising in terms of practice, because there is a lot of natural or artificial χG (NG): say, stars and their constellations. A precedent of such principle's usage can be found in [He, Vaidya, 1998].

A lot of confidential communication devices have advantages of steganography systems: for example, a message can be concealed by a chaotic signal in additive mixing mode. On the contrary, according to original idea, steganography systems are not obliged to save confidentiality in the working conditions of cryptography systems. It's natural that if confidentiality is lost, so it's not a cryptosystem.

3 Simulation of processes in generator of chaotic oscillations and its experimental implementation

Let's analyze a single-channel system of nonlinear-dynamic cryptography (without a dedicated synchronization line) with internal generator of deterministic chaos. Its schematic layout is depicted on Fig. 4, *a* at m=1. To implement such system it's suggested to use the following chaos generator (Fig. 6).

Let's describe (in rather abstract form) mathematical model of chaos generator. Let's $U_{out} \equiv U = f(U_{in})$ is a static transfer characteristic of the nonlinear element. Its time delay will be described in a phenomenological way by introducing τ_n relaxation time. Let's assume that matching devices and diodes have small time delay. So dynamics model in the chaos generator is:

$$\tau_n \partial U(t)/\partial t = -U(t) + f(U(t-t_e)), \qquad (1)$$

where t_e is a time lag in the feedback loop.

If $\tau_n \partial U(t)/\partial t \approx 0$ or $\tau_n << t_e$, then (1) model can be transformed into a discrete map:

$$U_{i+1} = f(U_i), \qquad (2)$$

where i is a discrete time.

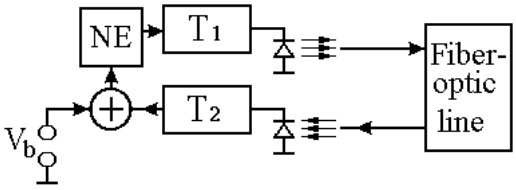

Figure. 6. Scheme of deterministic chaos generator for a cryptosystem: *NE* is a nonlinear element, T_1 and T_2 are matching devices (transformers), V_b is a bias voltage.

4 Nonlinear element with Λ-shaped static transfer characteristic and its mathematical description

Let's choose as a basis of nonlinear element a scheme of two complementary field-effect transistors (Fig. 7, *a* [Chua, Juebang, Youying, 1985] and [Kumar, 2002]). It's convenient to use the following function for approximation of its transfer characteristic $I_{\Lambda\,exp}(U)$:

$$y(x, x_0, y_0, x_1, y_1, \alpha_0, \alpha_1, M) = 0{,}5(y_1+y_0) - 0{,}5(y_1-y_0)\cdot\cos[\pi[(x-x_0)/(x_1-x_0)]^{\alpha}],$$

$$\alpha=\alpha(x, x_0, x_1, \alpha_0, \alpha_1, M)= =\alpha_0+(\alpha_1-\alpha_0)[(x-x_0)/(x_1-x_0)]^M,$$

where x_0, y_0, x_1, y_1, α_0, α_1, M are coefficients for the approximation, (x_0, y_0), (x_1, y_1) have the meaning of coordinates of two extremes of the approximating function. According to simulation, experimental characteristic $I_{\Lambda\,exp}(U)$ is approximated by $I_\Lambda(U)$ with $\langle|I_\Lambda(U)-I_{\Lambda\,exp}(U)|\rangle = 4{,}244\cdot10^{-6}$ A precision (Fig. 7, *b*), where

$$I_\Lambda(U)=\begin{cases} I_0, & U \le U_0 \\ y(U,U_0,I_0,U_1,I_1,1,1,0), & U_0 < U \le U_1 \\ y(U,U_1,I_1,U_2,I_2,\alpha_0,\alpha_1,M), & U_1 < U < U_2 \\ I_2, & U \ge U_2 \end{cases}, \qquad (3)$$

U_0=0,39 V, $I_0=4\cdot10^{-5}$ A, U_1=1,174 V, I_1=0,34053 A, U_2=3,935 V, $I_2=10^{-5}$ A, α_0=0,7, α_1=0,17, M=0,68.

Therefore it's possible to create a chaos generator (Fig. 8) on the basis of the nonlinear element (Fig. 7, *a*). Its model in the form of discrete map (2) contains approximation of current-voltage characteristic (3), which is depicted on Fig. 7, *b*:

$$U_{i+1} = R\, I_\Lambda(K(U_i+V)), \qquad (4)$$

where R is a resistance, K is a transfer coefficient of adder unit (Fig. 6).

To detect dynamics type in the model a difference between current value U_i ($10^4<i<10^6+10^4$) and previously been observed U_j ($j=10^4$) was controlled. If $|U_j-U_i|<10^{-40}$, then the regime was treated as periodic with period of $i-j$. To reduce influence of transient processes on map of regimes there was enough (10^4) free "warmup" iterations. Results of (4) model simulation are depicted on Fig. 9 and Fig. 10.

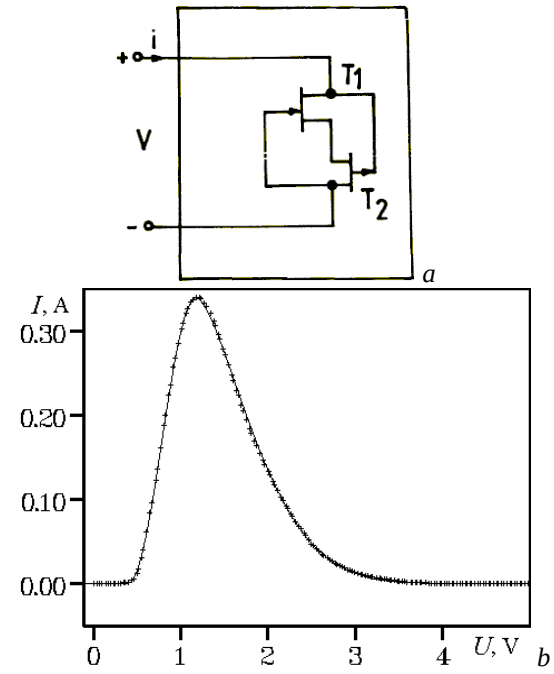

Figure. 7. Circuit configuration of a nonlinear element, which consists of two field-effect transistors (*a*) [Chua, Juebang, Youying, 1985] and [Kumar, 2002] and its Λ-shaped static current-voltage characteristic (*b*): experimental data is marked with "+", lines is the result of approximation.

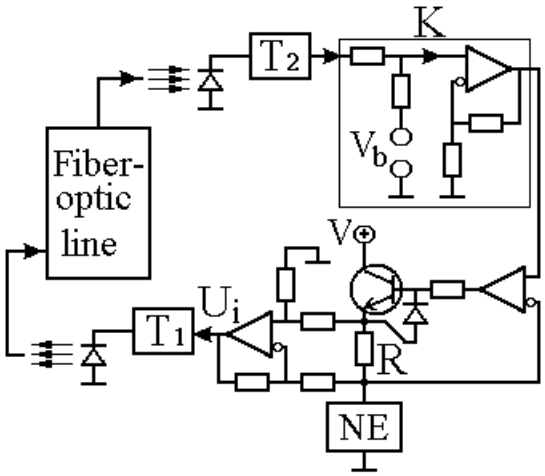

Figure. 8. Detailed scheme of deterministic chaos generator for a cryptosystem.

Concerning the recommendations on choise of model parameters of the chaos generator. It is considered, that for mentioned systems for maintenance of confidentiality of communication such parameters of the generator are favorable, at which the unpredictability of signal is maximum. According to Fig. 9 and Fig. 10 it's possible to conclude that negative values of amplification factor are also usable for purposes of creation of deterministic chaos generator. Regions of large periods are located close to the axis (Fig. 9), so to create a chaos generator it's enough to set small bias voltages (V_b=±5V) and mod-

erate amplification factor values (K~±15). According to Fig. 10 suitable values of resistance are R~(15...30) Ohms. Therefore parameters' estimation made on the basis of Fig. 9 and Fig. 10 is favorable for hardware implementation of the device. According to constructed maps there can be deterministic chaos mode in the (4) model. In its turn, it shows that a confidential communication system on the basis of chaos generator (Fig. 8) can be implemented.

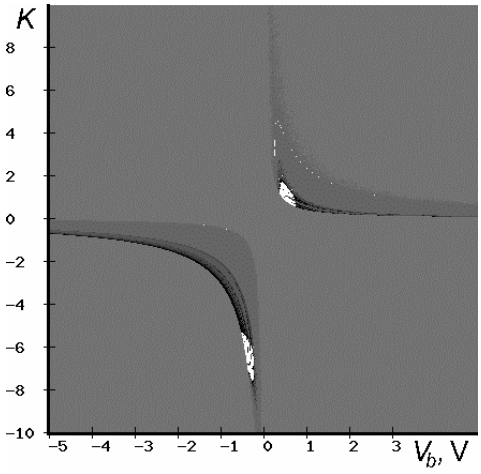

Figure. 9. Regimes map for (4) model in coordinates: bias voltage V_b – amplification factor K at R=6,7 Ohm, U_0=5 V. White color means non-periodic regimes, regular ones are grayscaled (darker regions corresponds to larger periods).

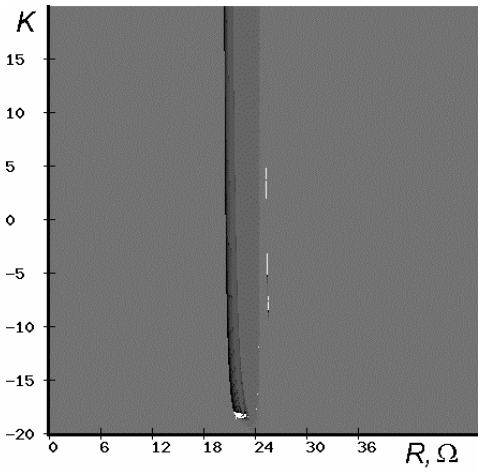

Figure. 10. Regimes map for (4) model in coordinates: resistance R – amplification factor K at V_b=–1 V, U_0=5 V. White color means non-periodic regimes, regular ones are grayscaled (darker regions corresponds to larger periods).

5 Conclusion

A classification of cryptosystems was developed by the authors. The classification basis is: a) position (relative to it) of chaos generator, b) decipherer working mode, c) number of communication channels, d) function of communication channel. The classification contains a number of new confidential communications systems. Heuristic potential of the proposed classification lets to perform meaningful development of cryptosystems on the basis of chaos generators (noise generators).

A variant of chaos generator, which combines radioelectronic and fiber-optic components, for a cryptosystem was introduced. A mathematical model of its dynamics was constructed. A version of the model in the form of discrete map was simulated; a number of dynamic regimes' maps was constructed on its basis. That maps let to find out which values of generator's parameters corresponds to periodical or non-regular oscillations. Results of performed simulation let to estimate technical parameters of the device and prove implementation possibility of confidential communication system on the basis of chaos generator.

References

Chua L., Juebang Yu., Youying Yu (1985) Bipolar-JFET-MOSFET negative resistance devices. *IEEE Transactions on circuits and systems.* **V 32**, № 1. P. 46–61.

Dmitriev A. S., Panas A. I. (2002) *Dynamical chaos: new information carriers for communication systems*. Moscow: Fizmatlit. 252 p. (in Russian).

Dmitriev A. S., Starkov S. O. (1998) Transmission of messages with the use of chaos and classical theory of information. *Foreign Radioelectronics.* N 11. P. 4–31. (in Russian).

He R., Vaidya P. G. (1998) Implementation of chaotic cryptography with chaotic synchronization. *Phys. Rev. E.* **V. 57**, № 2. P. 1532–1535.

Izmailov I. V., Lyachin A. V., Poizner B. N. (2007) *Deterministic chaos in models of nonlinear ring interferometer.* Tomsk: Publishing House of Tomsk State Univerity. 256 p. (in Russian)

Izmailov I. V., Poizner B. N. (2001) Variants of realization of nonlinear-optical device of confidential data transmission. *Atmospheric and Oceanic Optics.* **V. 14**, N 11. P. 1074–1086. (in Russian)

Kal'yanov E. V., Grigor'yants V. V. (2001) Data transmission with the use of masking chaotic oscillations. *Letters to ZHTF.* **V. 27**, N 6. P. 71–76. (in Russian).

Kumar U. (2002) A complication of negative resistance circuits generated by two novel algorithms. *Active and Passive Elec. Comp.* **V 25**. P. 211–214.

Vladimirov S. N., Izmailov I. V., Poizner B. N. (2008) *Nonlinear-dynamic cryptology: radiophysical and optical systems* / Ed. by S.N. Vladimirov. Moscow, Fizmatlit. (in press, in Russian).

Vladimirov S. N., Negrul V. V. (2000) Communication systems with passive chaotic synchronization. Proc. of 5th International Conference. In *Actual Problems of Electronic Instrument Engineering APEP-2000*. Novosibirsk, 26–29 of September, 2000. Novosibirsk. **V. 7**. P. 39–41. (in Russian).