Issues in IFS and GNs, Vol. 12, 2015/2016, 129–138

Generalized Net Model for Information Encryption by Chua and Neural Networks

Stanimir Surchev[1], **Sotir Sotirov**[1], **Maciej Krawczak**[2]

[1] Computer Systems and Technologies Department
"Prof. Assen Zlatarov" University
1 "Prof. Yakimov" Blvd., 8010 Burgas, Bulgaria
e-mails: ssurchev@gmail.com, ssotirov@btu.bg

[2] Systems Research Institute, Polish Academy of Sciences
Warsaw School of Information Technology, Warsaw, Poland
e-mail: krawczak@ibspan.waw.pl

Abstract: In this paper, a generalized net model of cryptographic method is described. The basic components for encryption and decryption of information are signals from Chua's circuit and Multilayer neural network.
Keywords and phrases: Neural network, Generalized net, Chua's circuit, Cryptography.
2000 Mathematics Subject Classification: 68Q85.

Introduction

Hiding information from an unauthorized person is a subject that is very important for everyone. Cryptography is a field that describes processes of encoding and decoding information. The main cryptographic methods are:

- Symmetric-key cryptography [2]
- Public-key cryptography [3]

The neural networks [5] are a powerful tool for processing complicate algorithms. They are used for complex encrypting methods [9, 10].

In this method, a Chua's circuit is used. It is an electrical circuit created by Chua and Matsumoto [4]. In Fig. 1, the electrical schematic of the circuit is presented.

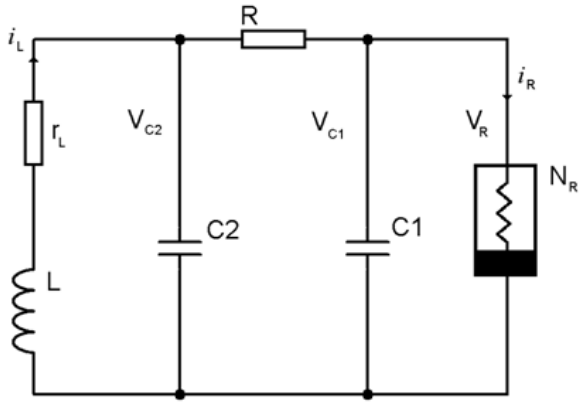

Figure 1. Electrical schematic of Chua's circuit

Chua's circuit is a simple scheme that is created by three passive components and one nonlinear component. For the aim of this paper an oscilloscope is used, that measures the voltage of capacitor C_2. The length of the measured signal is five seconds, which is 500 000 units. In Fig. 2, a part of measured signal is shown.

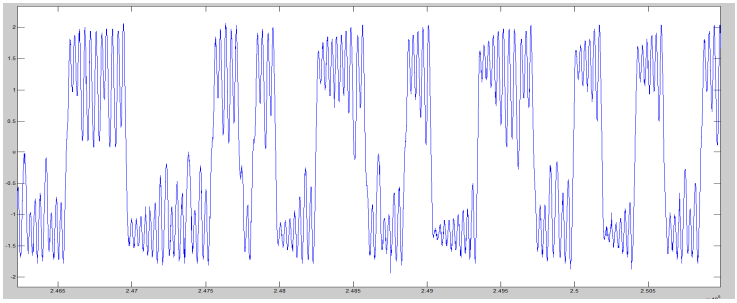

Figure 2. Part of the measured signal by oscilloscope

The measured values contain positive and negative peaks that create different intervals of time. A positive interval begins at a value greater than 0.2 and ends with a value less than -0.55, while the negative interval begins with a value less than -0.55 and ends with a value greater than 0.2. The calculated intervals have values between 0 and 1500. In Fig. 3 a part of the signal intervals is shown.

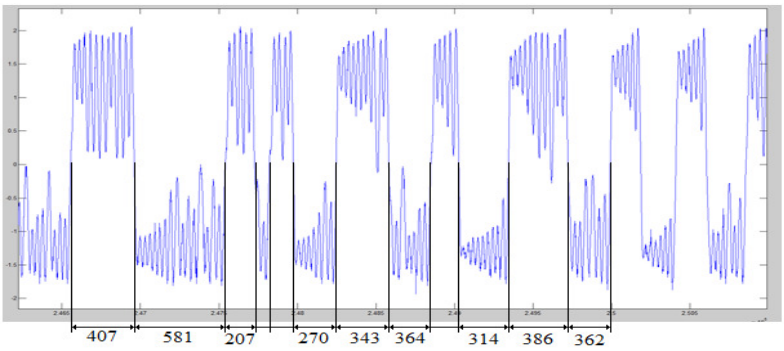

Figure 3. Positive and negative signal intervals

The group of intervals defines a different symbol (Table 1).

Table 1. Definition of symbols by group of intervals

Intervals	Symbol
361 to 390	C
391 to 420	H
271 to 300	U
571 to 600	A

The defined symbols are used to create input vectors and target vectors of a multilayer neural network (Fig. 4)

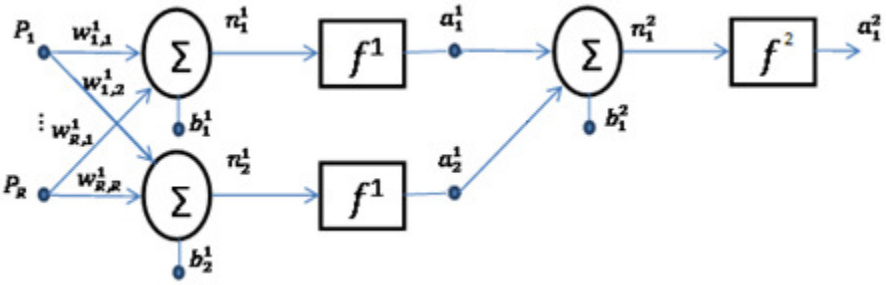

Figure 4. Multilayer neural network

When the training process of the neural network is complete, the next step is the selection of intervals for every symbol in the message. When this

operation is complete, it is necessary to determine their starting points. In Fig. 5, the encoding process of the message is shown.

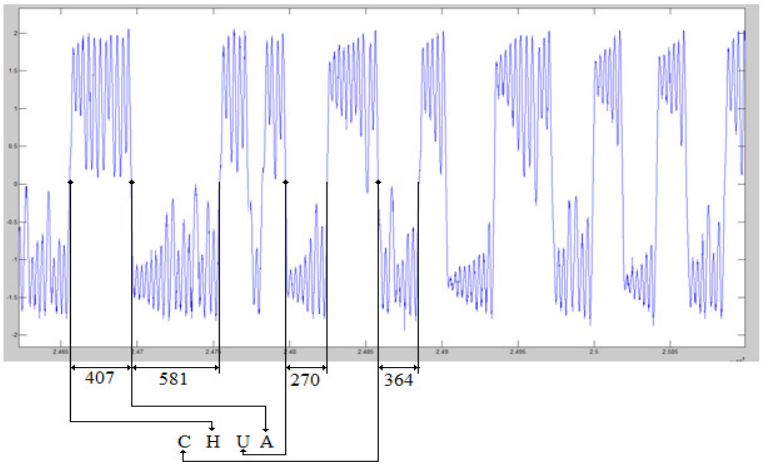

Figure 5. Starting point of the chosen intervals
for every symbol from the message

The last part is sending the following data to the other person:

- Chua's circuit signal
- Created Multilayer Neural Network
- Initial points for every symbol from the message

Generalized Net Model

There is many GM that are used for modelling different type of neural networks [11, 12].

Initially the following tokens enter the GN [1]. In place L_1 – α token with initial characteristics x_0^{α} = "Chua's circuit". In place L_6 – β token with initial characteristics x_0^{β} = "Neural network's parameters". In place L_7 – γ token with initial characteristics x_0^{γ} = "Test message". In place L_{13} – δ token with initial characteristics x_0^{γ} = "The message".

The GN is presented in Fig. 6 by the following set of transitions:

$$A = \{Z_1, Z_2, Z_3, Z_4\}$$

These transitions describe the following processes:

- Z_1 = “Generating and processing Chua signal”,
- Z_2 = “Creating and training Neural Network”,
- Z_3 = “Message encryption”,
- Z_4 = “Message decryption”.

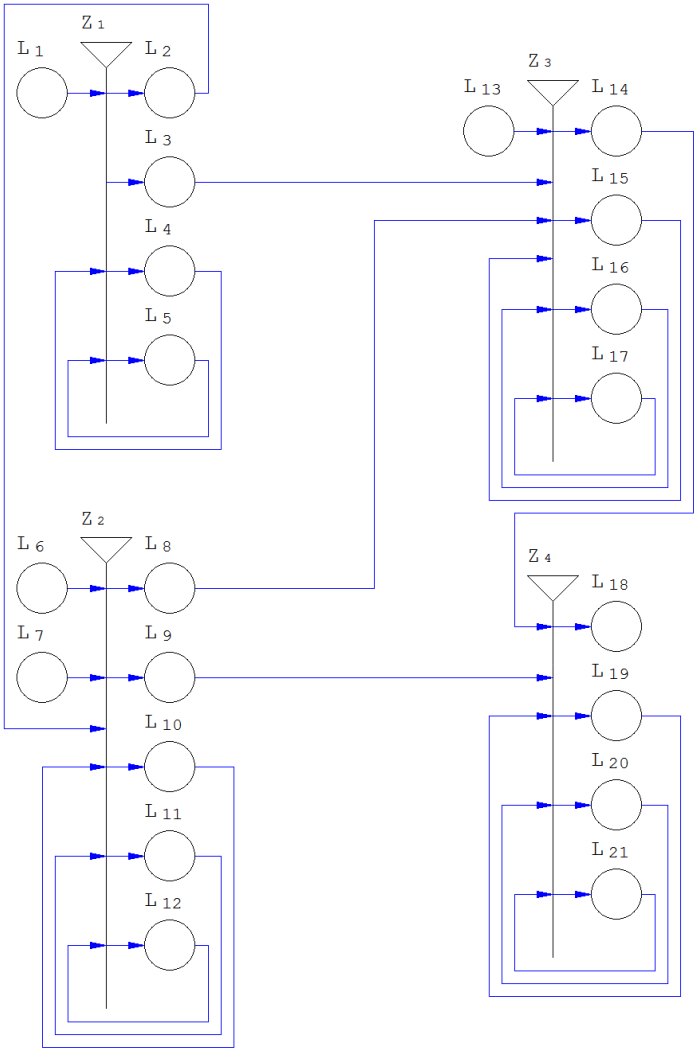

Figure 6. Generalized net model

$$Z_1 = \langle (L_1, L_4, L_5),(L_2, L_3, L_4, L_5), R_1, \vee(L_1, L_4, L_5)\rangle$$

$$R_1 = \begin{array}{c|cccc} & L_2 & L_3 & L_4 & L_5 \\ \hline L_1 & false & false & false & true \\ L_4 & W_{4,2} & W_{4,3} & true & false \\ L_5 & false & false & W_{5,4} & true \end{array}$$

where

- $W_{4,2}$ = $W_{4,3}$ = *"Positive and negative intervals of Chua's signal are calculated"*,
- $W_{5,4}$ = *"Chua's signal is generated"*.

The token α from place L_2 enters place L_5 with characteristics: x_{cu}^{α} = " $pr_1 x_{cu}^{\alpha}$, Chua's signal". Token α from place L_5 splits into two tokens:

- token α stays in place L_5 for the throughout the whole generalized net.
- token α' enters place L_4 and obtain new characteristics: $x_{cu}^{\alpha'}$ = "$\mathrm{pr}_2\, x_{cu}^{\alpha}$, Lengths of positive and negative intervals, Starting points of the intervals"

Tokens α' from place L_4 splits into two tokens:

- token α' enters place L_2 with characteristics: $x_{cu}^{\alpha'}$ = "$\mathrm{pr}_2\, x_{cu}^{\alpha'}$"
- token α' enters place L_3 with characteristics: $x_{cu}^{\alpha'}$ = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$"

$$Z_2 = \langle (L_2, L_6, L_7, L_{10}, L_{11}, L_{12}),(L_8, L_9, L_{10}, L_{11}, L_{12}), R_2, \vee(L_2, L_{11}, \wedge(L_6, L_{12}), \wedge(L_7, L_{11}))\rangle$$

$$R_2 = \begin{array}{c|ccccc} & L_8 & L_9 & L_{10} & L_{11} & L_{12} \\ \hline L_2 & false & false & false & false & true \\ L_6 & false & false & false & true & false \\ L_7 & false & false & true & false & false \\ L_{10} & W_{10,8} & W_{10,9} & true & W_{10,11} & false \\ L_{11} & fasle & false & W_{11,10} & true & false \\ L_{12} & false & false & false & W_{12,11} & true \end{array}$$

$W_{10,8}$ = $W_{10,9}$ ="Properly trained neural network",
$W_{10,11} = \neg W_{10,8}$,

$W_{11,10}$ = “Trained neural network”,
$W_{12,11}$ = ”Created input and target vectors”.

Token α' from place L_2 enters place L_{12} with characteristics: $x_{cu}^{\alpha'}$ = “$\mathrm{pr}_1 x_{cu}^{\alpha'}$, $\mathrm{pr}_2 x_{cu}^{\alpha'}$, $\mathrm{pr}_3 x_{cu}^{\alpha'}$, Input and target vectors”.

Tokens α' and β from place L_{12} and L_6 enter place L_{11} and they unite in a new token with characteristics: $x_{cu}^{\alpha''}$ = ”$\mathrm{pr}_1 x_{cu}^{\alpha'}$, $\mathrm{pr}_2 x_{cu}^{\alpha'}$, $\mathrm{pr}_3 x_{cu}^{\alpha'}$, $\mathrm{pr}_4 x_{cu}^{\alpha'}$, $\mathrm{pr}_1 x_{cu}^{\beta}$, Trained neural network”.

Tokens α'' and γ from place L_{11} and L_7 enter in place L_{10} and they unite in a token α''' with characteristics: $x_{cu}^{\alpha'''}$ = “$\mathrm{pr}_1 x_{cu}^{\alpha'}$, $\mathrm{pr}_2 x_{cu}^{\alpha'}$, $\mathrm{pr}_3 x_{cu}^{\alpha'}$, $\mathrm{pr}_4 x_{cu}^{\alpha'}$, $\mathrm{pr}_1 x_{cu}^{\beta}$, $\mathrm{pr}_6 x_{cu}^{\alpha''}$, Tested neural network”.

Token α''' from place L_{10} enters in place L_{11} with characteristics: $x_{cu}^{\alpha''''}$ = “$\mathrm{pr}_1 x_{cu}^{\alpha'}$, $\mathrm{pr}_2 x_{cu}^{\alpha'}$, $\mathrm{pr}_3 x_{cu}^{\alpha'}$, $\mathrm{pr}_4 x_{cu}^{\alpha'}$, $\mathrm{pr}_1 x_{cu}^{\beta}$, $\mathrm{pr}_6 x_{cu}^{\alpha''}$, $\mathrm{pr}_7 x_{cu}^{\alpha''''}$ = incorrectly trained”.

Token α''' from place L_{10} enters in place L_8 or L_9 with characteristics: $x_{cu}^{\alpha''''}$ = “$\mathrm{pr}_1 x_{cu}^{\alpha'}$, $\mathrm{pr}_2 x_{cu}^{\alpha'}$, $\mathrm{pr}_3 x_{cu}^{\alpha'}$, $\mathrm{pr}_4 x_{cu}^{\alpha'}$, $\mathrm{pr}_1 x_{cu}^{\beta}$, $\mathrm{pr}_6 x_{cu}^{\alpha''}$, $\mathrm{pr}_7 x_{cu}^{\alpha''''}$ = properly trained”.

$$Z_3 = \langle (L_3, L_8, L_{13}, L_{15}, L_{16}, L_{17},), (L_{14}, L_{15}, L_{16}, L_{17}), R_3, \vee(L_{15}, L_{16}, L_{17}, \wedge(L_3, L_8, L_{13})) \rangle$$

R_3 =

	L_{14}	L_{15}	L_{16}	L_{17}
L_3	*false*	*false*	*false*	*true*
L_8	*false*	*false*	*false*	*true*
L_{13}	*false*	*false*	*false*	*true*
L_{15}	*false*	*true*	$W_{15,16}$	*false*
L_{16}	$W_{16,14}$	$W_{16,15}$	*true*	*false*
L_{17}	*false*	$W_{17,15}$	*false*	*true*

$W_{16,14}$ = “Properly encrypted message”,
$W_{16,15}$ = $\neg W_{16,14}$,
$W_{15,16}$ = “Encrypted message”,
$W_{17,15}$ = “The data for encryption are collected”.

Tokens α', α''' and δ from places L_3, L_8 and L_{13} enter place L_{17}. They unite in one token ε with characteristics: x_{cu}^{ε} = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$, $\mathrm{pr}_4\, x_{cu}^{\alpha'}$, $\mathrm{pr}_1\, x_{cu}^{\beta}$, $\mathrm{pr}_6\, x_{cu}^{\alpha''}$, $\mathrm{pr}_7\, x_{cu}^{\alpha'''}$, $\mathrm{pr}_1\, x_{cu}^{\delta}$, Encryption data".

Token ε from place L_{17} enters place L_{15} and obtains new characteristic: x_{cu}^{ε} = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$, $\mathrm{pr}_4\, x_{cu}^{\alpha'}$, $\mathrm{pr}_1\, x_{cu}^{\beta}$, $\mathrm{pr}_6\, x_{cu}^{\alpha''}$, $\mathrm{pr}_7\, x_{cu}^{\alpha'''}$, $\mathrm{pr}_1\, x_{cu}^{\delta}$, $\mathrm{pr}_9\, x_{cu}^{\varepsilon}$, Encrypted message".

Token ε from place L_{15} enters place L_{16} and obtains new characteristic: x_{cu}^{ε} = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$, $\mathrm{pr}_4\, x_{cu}^{\alpha'}$, $\mathrm{pr}_1\, x_{cu}^{\beta}$, $\mathrm{pr}_6\, x_{cu}^{\alpha''}$, $\mathrm{pr}_7\, x_{cu}^{\alpha'''}$, $\mathrm{pr}_1\, x_{cu}^{\delta}$, $\mathrm{pr}_9\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{10}\, x_{cu}^{\varepsilon}$, Tested encrypted message".

Token ε from place L_{16} enters place L_{15} with characteristics: x_{cu}^{ε} = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$, $\mathrm{pr}_4\, x_{cu}^{\alpha'}$, $\mathrm{pr}_1\, x_{cu}^{\beta}$, $\mathrm{pr}_6\, x_{cu}^{\alpha''}$, $\mathrm{pr}_7\, x_{cu}^{\alpha'''}$, $\mathrm{pr}_1\, x_{cu}^{\delta}$, $\mathrm{pr}_9\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{10}\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{11}\, x_{cu}^{\varepsilon}$ = incorrectly".

Token ε from place L_{16} enters place L_{14} with characteristics: x_{cu}^{ε} = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$, $\mathrm{pr}_4\, x_{cu}^{\alpha'}$, $\mathrm{pr}_1\, x_{cu}^{\beta}$, $\mathrm{pr}_6\, x_{cu}^{\alpha''}$, $\mathrm{pr}_7\, x_{cu}^{\alpha'''}$, $\mathrm{pr}_1\, x_{cu}^{\delta}$, $\mathrm{pr}_9\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{10}\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{11}\, x_{cu}^{\varepsilon}$ = properly".

$$Z_4 = \langle (L_9, L_{14}, L_{19}, L_{20}, L_{21}), (L_{18}, L_{19}, L_{20}, L_{21}), R_4, \vee(L_{19}, L_{20}, L_{21}, \wedge(L_9, L_{14})) \rangle$$

$R_4 =$

	L_{18}	L_{19}	L_{20}	L_{21}
L_9	*false*	*false*	*false*	*true*
L_{14}	*false*	*false*	*false*	*true*
L_{19}	$W_{19,18}$	*true*	*false*	*false*
L_{20}	*false*	$W_{20,19}$	*true*	*false*
L_{21}	*false*	*false*	$W_{21,20}$	*true*

$W_{19,18}$ = "Decrypted data are tested by the neural network",
$W_{20,19}$ = "Decrypted message",
$W_{21,20}$ = "Data for decryption process are collected".

Tokens α''' and ε from places L_9 and L_{14} enter place L_{21} and they unite in one token ε' with characteristics: $x_{cu}^{\varepsilon'}$ = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$, $\mathrm{pr}_4\, x_{cu}^{\alpha'}$, $\mathrm{pr}_1\, x_{cu}^{\beta}$, $\mathrm{pr}_6\, x_{cu}^{\alpha''}$, $\mathrm{pr}_7\, x_{cu}^{\alpha'''}$, $\mathrm{pr}_1\, x_{cu}^{\delta}$, $\mathrm{pr}_9\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{10}\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{11}\, x_{cu}^{\varepsilon}$, Collected data for decryption process".

Token ε' from place L_{21} enters place L_{20} and obtain new characteristic: $x_{cu}^{\varepsilon'}$ = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$, $\mathrm{pr}_4\, x_{cu}^{\alpha'}$, $\mathrm{pr}_1\, x_{cu}^{\beta}$, $\mathrm{pr}_6\, x_{cu}^{\alpha''}$, $\mathrm{pr}_7\, x_{cu}^{\alpha'''}$, $\mathrm{pr}_1\, x_{cu}^{\delta}$, $\mathrm{pr}_9\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{10}\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{11}\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{12}\, x_{cu}^{\varepsilon'}$, Decrypted data".

Token ε' from place L_{20} enters place L_{19} and obtains new characteristic: $x_{cu}^{\varepsilon'}$ = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$, $\mathrm{pr}_4\, x_{cu}^{\alpha'}$, $\mathrm{pr}_1\, x_{cu}^{\beta}$, $\mathrm{pr}_6\, x_{cu}^{\alpha''}$, $\mathrm{pr}_7\, x_{cu}^{\alpha'''}$, $\mathrm{pr}_1\, x_{cu}^{\delta}$, $\mathrm{pr}_9\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{10}\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{11}\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{12}\, x_{cu}^{\varepsilon'}$, $\mathrm{pr}_{13}\, x_{cu}^{\varepsilon'}$, Decrypted message".

Token ε' from place L_{19} enters place L_{18} and obtains new characteristic: $x_{cu}^{\varepsilon'}$ = "$\mathrm{pr}_1\, x_{cu}^{\alpha'}$, $\mathrm{pr}_2\, x_{cu}^{\alpha'}$, $\mathrm{pr}_3\, x_{cu}^{\alpha'}$, $\mathrm{pr}_4\, x_{cu}^{\alpha'}$, $\mathrm{pr}_1\, x_{cu}^{\beta}$, $\mathrm{pr}_6\, x_{cu}^{\alpha''}$, $\mathrm{pr}_7\, x_{cu}^{\alpha'''}$, $\mathrm{pr}_1\, x_{cu}^{\delta}$, $\mathrm{pr}_9\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{10}\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{11}\, x_{cu}^{\varepsilon}$, $\mathrm{pr}_{12}\, x_{cu}^{\varepsilon'}$, $\mathrm{pr}_{13}\, x_{cu}^{\varepsilon'}$, $\mathrm{pr}_{14}\, x_{cu}^{\varepsilon'}$, Visualization of message".

Conclusion

A cryptographic method, utilizing generalized net, is described in the present paper. It uses the generated signal from an electric scheme – Chua's circuit. The decoding process is carried out by a multilayer neural network. Generalized nets are a suitable tool for modeling intuitive and "smart" systems such as neural networks, as well as training based on professional and emotional foundation [6, 7]. On the other hand, the chaotic Chua scheme can recreate not only conditions for a realization with a neural network but also generate possible scenarios supporting the research on risk in maritime transport [8].

Acknowledgments

The authors are thankful for the support provided by the Bulgarian National Science Fund under Grant Ref. No. DN 02/10 "New Instruments for Knowledge Discovery from Data, and their Modelling".

References

[1] Atanassov K, *Generalized Nets*, World Scientific, Singapore, 1991.

[2] Diffie W., M. Hellman, New Direction in Cryptography, *IEEE Transitions on Information Theory*, Vol. IT-22, Nov. 1976, 644–654.

[3] Diffie, W., M. Hellman, Multi-user cryptographic techniques. *AFIPS Proceedings* 45, 1976, 109–112.

[4] Matsumoto, T., L. O. Chua and M. Komuro. The double scroll. *IEEE Trans. on Circuits & Syst.*, CAS-32(8), 1985, 797–818,

[5] McCulloch, P. Walter, A logical calculus of the ideas immanent in nervous activity, *Bulletin of Mathematical Biophysics*, Vol. 5, 1943, 115–133.

[6] Vankov, P., Vankova, D. Experience – Based Innovative Programme in Varna, Bulgaria. *Education & Professional Development of Engineers in the Maritime Industry*, 9–10 December, London, UK, The Royal Institution of Naval Architects, 23–26.

[7] Vankov, P., Vankova, D. Sustainable Educational & Emotional Model – An Experience from Bulgaria. Pr*oceedings of Edulearn 15 Conference*, 6-8 July 2015, Barcelona, Spain, 1600–1605.

[8] Vankov, P. Freight Containers Maritime Transportation' Risks – Research Experience and Future Perspectives, *Proceedings of Twelfth International Conference on Marine Sciences and Technologies*, September 25-27, 2014, 170–172.

[9] Volná, E., Using Neural network in cryptography. The State of the Art in Computational Intelligence, 2000, 262–267.

[10] Wolfgang Kinzel and Ido Kanter, Interacting neural networks and cryptography, Advances in Solid State Physics, Ed. by B. Kramer, Springer, Berlin, 2002, Vol. 42, p. 383.

[11] Sotirov S, V. Kukenska, M. Hristova, I. Vardeva, L. Staneva, J. Barzov, S. Dimitrov, S. Stoqnova, Modeling the nonlinear auto-regressive network with exogenous inputs with generalized net, *Development in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics. Vol II: Applications*, System Research Institute, Polish Academy of Science. Warsaw, 2010, 223–230.

[12] Petkov T., S. Sotirov, Generalized net model of slow learning algorithm of unsupervised ART2 neural network, *Proc. of Twelfth International Workshop on Intuitionistic Fuzzy Sets and Generalized Nets (IWIFSGN'2013)*, Warsaw, 2014, 61–70.