# 11th International Conference


# New Electrical and Electronic Technologies and their Industrial Implementation

Zakopane, Poland, June 25 – 28, 2019

Edited by **Tomasz N. Kołtunowicz**

ISBN: 978-83-7947-369-4

Publisher: Lublin University of Technology
20-618 Lublin, 38d Nadbystrzycka Str.
Realization: Lublin University of Technology Library
e-mail: wydawca@pollub.pl

# Probabilistic measure of space for neurocryptographic system solutions

**P. Urbanovich[1,2], D. Karczmarski[2], M. Płonkowski[2]**
[1] *Belarusian State Technological University, Minsk, Belarus*
[2] *Lublin Catholic University, Lublin, Poland, E-mail: pav.urb@yandex.by, dominik@karczmarski.com*

The cryptographic key matching can be based on artificial neural network technologies. Kinzel-Kanter protocol uses neural networks (*A* and *B*) ability in mutual learning and generating common secret key [1]. This idea was developed (in particular, see [2-4]). In this report a probabilistic approach that combines network parameters and the time of their synchronization is analyzed. Each neurocryptographic net (machine, *PM*) defines three values: *K*, *N*, *L*. We're talking about a two-layer neural network. In the entrance layer we have *K* neurons. Each of these neurons has *N* inputs. Let $w_{ij}$ ($i$ = 1,2, ..., *K*) be the weight vector for the neuron with index *i*. Let *j* be the weight for the entry with the index j in the neuron with the index *i*. Each of the weights can assume a value between ⟨-*L*; *L*). We analyze the neurocryptographic machine *PM*(*K*, *N*, *L*). The set of the initial values of weights is the set: $\langle -L;+L\rangle^N \times \langle -L;+L\rangle^N \times ... \times \langle -L;+L\rangle^N$, being the Cartesian product of the *K* same collections. Without reducing the generality of the task (determining of the space size) we can deal with determining the size of space $\langle -L;+L\rangle^N$ only for one neuron. In literature the safe PM key exchange system is considered to be where *N*>100. For such a large *N* value, the exact determination of the space dimension (within a reasonable time) is computationally not possible. Therefore, another way to determine the size of the space should be introduced. Probability value $|PM(K, N, L)|_P$ that the randomly selected point in the synchronization process of *A* and *B* sets will be compatible with the solution can be a measure of the space size. Due to the possibility of determining of the space size, you can explore and appropriately chosen values of *K*, *N*, *L*. While intuitively it seems that increasing the value of parameters is proportional to the strength of the system, it is not so obvious which of the systems is better: *PM*(*K*=3, *N*=20, *L*=5) or *PM*(*K*=3, *N*=15, *L*=10). 100 tests completed. In each test points were randomly selected until 10 correct solutions were found among them, i.e. points which in the synchronization process were correct solutions. The following table shows some of the results.

| Parameters: *K*, *N*, *L* | Average of $\|.\|_P$ for one neuron | Average of $\|.\|_P$ for the whole |
|---|---|---|
| (*K*=3, *N*=40, *L*=5) | 0.025100000206 | 0.000015625 |
| (*K*=6, *N*=40, *L*=5) | 0.28698 | 0.00055861 |

## References

[1] Kinzel W., Kanter I.: Interacting neural networks and cryptography, [Electronic resource], 2002. Mode of access: http://theorie.physik.uni-wuerzburg.de/~ruttor/neurocrypt.html.
[2] Плонковски М., Урбанович П.П.: Криптографическое преобразование информации на основе нейросетевых технологий/ Труды БГТУ. Серия VI. Физико-математические науки и информатика, Минск: БГТУ, 2005, Вып.XIII, с.161–164.
[3] Urbanovich P.P., Lisitsa E.L.: Software for modeling the neural-cryptographic system/ New Electrical and Electronic Technologies and their Industrial Implementation: Proc. of the 6-th Intern. Conf. NEET'2009., Zakopane, Poland. Lublin, 2009, p. 57.
[4] Urbanowicz P., Kozera R, Dolecki M.: Zastosowanie sztucznych sieci neuronowych do uwzgledniania kluczy kryptograficznych. Ksiega pomiątkowa ku czci Księdza Profesora Andrzeja Szostka MIC, Lublin: KUL, 2016, p. 489-496.