Edited by **Tomasz Kołtunowicz**

Cover design by **Mariusz Kolasik**

Published with consent of Rector
of Lublin University of Technology

ISBN 978-83-7497-074-7

Lublin University of Technology Press
20-109 Lublin, 13 Bernardyńska Str.
e-mail:wydawnictwo@pollub.pl

Print: Printing House Ex-libris
20-484 Lublin, 3 Inżynierska Str.

INTERNATIONAL SCIENTIFIC COMMITTEE

Paweł Żukowski	Lublin University of Technology, Poland – **Chairman**
Vladimir Odzhaev	Belarussian State University, Belarus – **Co-Chairman**
Liudvikas Pranevicius	Vytautas Magnus University, Lithuania – **Co-Chairman**
Fiodor Romaniuk	Belarussian State Technical University, Belarus – **Co-Chairman**
Dmitro Freik	Precarpathian University, Ukraine – **Co-Chairmans**
Igor Tashlykov	Belarussian State Pedagogical University, Belarus – **Co-Chairman**
Janusz Partyka	Lublin University of Technology, Poland – **Scientific Secretary**
Viktor Anischik	Belarussian State University, Belarus
Guennadi Bondarenko	Moscow State Institute of Elektronics and Mathematics, Russia
Tomasz Boczar	Technical University of Opole, Poland
Kazimierz Cywiński	Bialystok Technical University, Poland
Zbigniew Gacek	Silesian University of Technology, Poland
Alfonsas Grigonis	Kanaus University of Technology, Lithuania
Jeon Han	Sung Kyun Kwan University, Korea
Czesław Karwat	Lublin University of Technology, Poland
Stas Kharin	Mathematic Institute of Kazakhstan Academy of Science, Kazakhstan
Sergei Kislitsin	Institute of Nuclear Physics, Kazakhstan
Fadiej Komarov	Belarussian State University, Belarus
Zbigniew Kowalski	Wroclaw University of Technology, Poland
Dariusz Mączka	M.Curie-Sklodowska University, Poland
Bogdan Miedziński	Wroclaw University of Technology, Poland
Franciszek Mosiński	Technical University of Lodz, Poland
Hassan Nouri	University of the West of England, United Kingdom
Aleksy Patryn	Technical University of Koszalin, Poland
Wiktor Pietrzyk	Lublin University of Technology, Poland
Vladimir Philipenko	RPC Integral, Minsk, Belarus
Alexander Pogrebnjak	Sumy Institute of Surface Modification, Ukraine
Jerzy Skubis	Technical University of Opole, Poland
Ryszard Smarzewski	Catholic University of Lublin, Poland
Jan Subocz	Technical University of Szczecin, Poland
Lech Subocz	Technical University of Szczecin, Poland
Aleksander Tadzhibaev	Petersburg Power Engineering Training Institute for Managers and Experts, Russia
Piotr Tarkowski	Lublin University of Technology, Poland
Yuri Tyurin	Electric Welding Institute NANU, Ukraine
Roland Wiśniewski	Institute of Atomic Energy, Poland
Waldemar Wójcik	Lublin University of Technology, Poland
Jerzy Zdanowski	Wroclaw University of Technology, Poland
Jerzy Żuk	M.Curie-Sklodowska University, Poland

LOCAL ORGANIZING COMMITTEE

Paweł Węgierek	Lublin University of Technology – **Chairman**
Mariusz Kolasik	Lublin University of Technology
Tomasz Kołtunowicz	Lublin University of Technology
Czesław Kozak	Lublin University of Technology
Zenon Pawełczak	Lublin University of Technology
Mirosław Pawłot	Lublin University of Technology
Wiktor Pyda	Lublin University of Technology
Barbara Skalska	Lublin University of Technology

Software for modeling the neural-cryptographic system

P.P. Urbanovich[1,2], E.L. Lisitsa[1]
[1] *Belorussian State Technological University, Minsk, Belarus, e.lisitsa@tut.by*
[2] *Lublin Catholic University, Lublin, Poland*

This report is devoted to a description of software for modeling cryptographic system which is based on neural networks technology. Kinzel-Kanter protocol uses neural networks ability in mutual learning and generating common secret key [1]. In this way Kinzel-Kanter protocol solves the main problem of symmetric system - keys' distribution, since it can provide the safety exchange between sender and recipient.

The main goal of software implementation is granting the ability of experimental studying, rating its performance, reliability and safety at various parameters (learning rules, the number of perceptrons and inputs, synaptic depth limits) of neural network protocol. Besides that 3 kinds of attack (simple, geometric and majority-geometric) were applied [3].

In software was implemented the standard Kinzel-Kanter architecture: each party uses a two level neural network (TPM). The first level contains K independent perceptrons, while the second level computes the parity of their K hidden outputs. Each one of the K perceptrons has N weights $w_{k,n}$ (where $1 \le k \le K$ and $1 \le n \le N$). These weights are integers in the range {-L,...,L} that can change overtime. Given the N bit input ($x_{k,1}, x_{k,2}, \ldots, x_{k,n}$), (where $x_{k,n} \in \{-1, 1\}$), the perceptron outputs the sign (which is also in {–1, 1}) of scalar product of inputs and the weights. The values of this outputs pass through the threshold activity function and the final output bit of each TPM is defined by the product of the hidden units. Both partners initialize their weight vectors by means of random numbers before the training period starts. At each time step a public input vector is generated and the final output bits are exchanged over the public channel. In the case of identical output bits, each TPM adjusts those of its weights for which the hidden unit is identical to the output. These weights are adjusted according to a given learning rule. The following learning rules were applied: Hebbian rule, anti-Hebbian rule, Random walk and Hebbian modification rule that was found experimentally and shows high level of safety. After some time two partners are synchronized and the communication is stopped. The common weight vector is used as a key to encrypt secret messages. The simple example of encryption/decryption process was also implemented in software.

With the help of software the following results of researches were obtained [3]. Kinzel-Kanter protocol is safe when simple attack is used. For providing the safety from geometric and majority-geometric attacks reasonably to use Hebbian modification rule and synaptic depth more than 4.

References

[1] W. Kinzel, I. Kanter: *Interacting neural networks and cryptography*, [Electronic resource], 2002, – Mode of access: http://theorie.physik.uni-wuerzburg.de/~ruttor/neurocrypt.html
[2] A. Klimov, A. Mityagine: *Analysis of Neural Cryptography*, [Electronic resource], 2003, Mode of access: http://theorie.physik.uni-wuerzburg.de/~ruttor/neurocrypt.html
[3] D. Karchmarski, M. Plonkovski, E. Lisitsa: *Methods and algorithms of modeling cryptographic systems based on neural networks technologies* - D. Karchmarski, Proc. of the BSTU, Proc. of the BSTU, 2008, p. 137-140