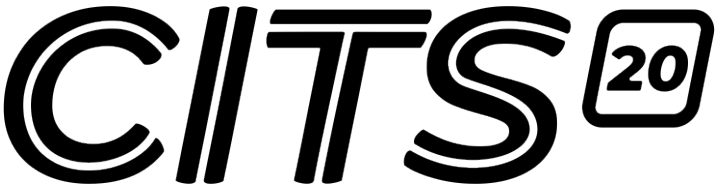

The 2020 International Conference on Computational Intelligence, Information Technology and Systems Research

Lublin University of Technology

December 17-20, 2020

Program Committee

Organizing Committee

Witold Pedrycz (University of Alberta, Canada; Systems Research Institute PAS, Warsaw, Poland)
Małgorzata Charytanowicz (Lublin University of Technology, Poland; Systems Research Institute PAS, Poland)
Dariusz Czerwiński (Lublin University of Technology, Poland)
Paweł Karczmarek (Lublin University of Technology, Poland)
Edyta Łukasik (Lublin University of Technology, Poland)
Marek Miłosz (Lublin University of Technology, Poland)
Elżbieta Miłosz (Lublin University of Technology, Poland)
Marcin Badurowicz (Lublin University of Technology, Poland)
Jacek Kęsik (Lublin University of Technology, Poland)
Adam Kiersztyn (Lublin University of Technology, Poland)
Magdalena Latkowska (Lublin University of Technology, Poland)
Paweł Powroźnik (Lublin University of Technology, Poland)
Tomasz Rybotycki (Systems Research Institute PAS, Warsaw, Poland)
Maria Skublewska-Paszkowska (Lublin University of Technology, Poland)
Jakub Smołka (Lublin University of Technology, Poland)
Stanisław Skulimowski (Lublin University of Technology, Poland)
Waldemar Suszyński (Lublin University of Technology, Poland)

3. The Stanford Natural Language Processing Group // http://nlp.stanford.edu/software/CRF-NER.html: 19.08.2020.

4. Rakhimova D., Turganbayeva A. Approach to Extract Keywords and Keyphrases of Text Resources and Documents in the Kazakh Language // In: Nguyen N.T., Hoang B.H., Huynh C.P., Hwang D., Trawiński B., Vossen G. (eds) Computational Collective Intelligence. ICCCI 2020. Lecture Notes in Computer Science, vol 12496. Springer, Cham. https://doi.org/10.1007/978-3-030-63007-2_56

The use of new technologies in cryptanalysis

December 19
9:30

Salamat Zhunusbayeva[1], Zhanna Alimzhanova[1]
[1]Al-Farabi Kazakh National University
71 al-Farabi Ave., Almaty, Kazakhstan
ssdarhan@gmail.com

The problem of protecting information resources is now becoming increasingly important. The report provides an overview of modern methods of cryptanalysis, namely, the use of genetic algorithms as a tool for recognizing encryption algorithms. A number of quantum cryptanalysis algorithms are also analyzed. Their computational complexity is compared with the computational complexity of similar classical algorithms. It is concluded that if practical examples of a quantum computer appear, modern asymmetric encryption systems will need to be improved and modified.

Key words: neural networks, cryptanalysis, gene algorithm, ciphers, quantum computers, cryptography, cryptographic security.

References

1. Spillman R., Janssen M., Nelson B., Kepner M. Use of a Genetic Algorithm in the Cryptanalysis of Simple Substitution Ciphers // Cryptologia. 17(1), 1993. P. 31-44.

2. Spillman R. Cryptanalysis of knapsack ciphers using genetic algorithms // Cryptologia, 17(1), 1993.

3. Saito A., Kioi K., Akagi Y., Hashizume N., Ohta K. Actual computational time-cost of the Quantum Fourier Transform in a quantum computer using nuclear spins. // Quantum Physics, abstract quant-ph/0001113

4. Matthews R. The use of genetic algorithms in cryptanalysts // Cryptologia. 17(2), 1993.

5. Shor P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // In Proceedings, 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, November 20–22, 1994, IEEE Computer Society Press. P. 124–134.

Author Index

Ślot, K., 3
Łuczak, P., 3
Łukasik, E., 4, 9, 12

Akkozov, A., 19
Alimzhanova, Z., 17, 18

Bakasova, P., 13
Bekmanova, G., 25

Charytanowicz, M., 4, 22
Czabak-Garbacz, R., 2
Czerwiński, D., 2

Danielewicz, A., 2

Fatyga, M., 2

Israilova, N., 13

Jędrzejewska-Rzezak, P., 7
Jaramillo-Alcázar, A., 11
Jaworski, T., 3

Kaczorowska, M., 4, 6
Kaderkeyeva, Z., 25
Kamiński, M., 2
Karczmarek, P, 7
Kiersztyn, A., 7
Kiersztyn, K., 7
Kucharski, J., 3
Kucharski, P., 3

Latalski, M., 2
Lolaev, M. Y., 20
Luján-Mora, S., 11, 23

Madrakhimov, S. F., 21
Makharov, K. T., 21
Milosz, M., 14
Miłosz, M., 4
Murzabekov, Z., 14

Nazarbayev, D., 18
Nazyrova, A., 25

Oruzbaeva, G., 19

Pabisz, M., 2
Pedrycz, W, 7
Perenc-Puchalska, I., 3
Plechawska-Wójcik, M., 6
Powroznik, P., 9

Rakhimova, D., 16

Sharsheeva, K., 19, 20
Skublewska-Paszkowska, M., 9, 12
Smołka, J., 12
Stęgierski, R., 22
Suleimenova, A., 16
Suszyński, W., 22

Tokovarov, M., 4, 6
Tultemirova, G., 19, 20
Turganbayeva, A., 16
Tussupova, K., 14

Wang, D., 1
Wawrzyk, M., 6

Zhunusbayeva, S., 17