

TERNOPIL NATIONAL ECONOMIC UNIVERSITY, UKRAINE
DEGGENDORF INSTITUTE OF TECHNOLOGY, GERMANY
UNIVERSITY OF SOUTH BOHEMIA, CZECH REPUBLIC
IEEE GERMANY SECTION / COMMUNICATIONS SOCIETY GERMAN
CHAPTER (COM19)

2020 10th International Conference on
**ADVANCED COMPUTER
INFORMATION TECHNOLOGIES
ACIT'2020**

Conference Proceedings

Deggendorf, Germany
September 16-18, 2020

2020 10th International Conference on Advanced Computer Information Technologies

ACIT'2020

Organized by:

Ternopil National Economic University, Ukraine
Deggendorf Institute of Technology, Germany
University of South Bohemia, Czech Republic
IEEE Czechoslovakia Section
IEEE Germany Section / Communications Society German Chapter (COM19)

Copyright and Reprint Permission:

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Operations Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331 or email to pubs-permissions@ieee.org.

To find more information about the IEEE policy visit www.ieee.org. Any person who believes that he or she has been the victim of illegal discrimination or harassment should contact IEEE Staff Director - Human Resources, at nondiscrimination@ieee.org or +1 732 465 6434.

IEEE Catalog Numbers

ISBN: 978-1-7281-6760-2

Part Number: CFP20S92-ART

**Copyright © 2020 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved.**

CONTENTS

SECTION 1

Mathematical Models of Objects and Processes

Packing Irregular Polygons using Quasi Phi-functions.....	1
<i>Alexandr Pankratov, Tatiana Romanova, Sergey Shekhovtsov, Igor Grebennik and Julia Pankratova</i>	
MRAC Implementation for Electric Throttle Valve	6
<i>Alireza Tajafari Sahebi, Amir Samiee and László Juhász</i>	
Integer Model of a Hexagonal Close-Packed Crystal Lattice and Calculation of the Number of Bonds Broken by an Arbitrary Plane	13
<i>Alla Savchenko, Alexey Galuza, Alla Belyaeva and Ivan Kolenov</i>	
Modeling of Soil Basis of Headed Hydrotechnical Structure’s Deformations Under Action Of Filtration Water Flow	18
<i>Anatoliy Vlasyuk, Mykola Kuzlo, Nataliia Zhukovska, Viktor Zhukovskyy and Nataliia Tarasyuk</i>	
Parallel Computing Optimization of Two-Dimensional Mathematical Modeling of Contaminant Migration in Catalytic Porous Media.....	23
<i>Anatoliy Vlasyuk, Viktor Zhukovskyy, Nataliia Zhukovska and Serhii Shatnyi</i>	
Modeling of Biological Wastewater Treatment Process Taking into Account Reverse Effect of Concentration on Diffusion Coefficient	29
<i>Andrii Safonyk, Viktor Zhukovskyy and Anna Burduk</i>	
Method of Automatic Rhythmcardiogram Formation with the Increased Informativeness by Means of the Electrocardiogram Processing	35
<i>Andriy Zozulia, Iaroslav Lytvynenko, Nadiia Lutsyk, Serhii Lupenko and Oleh Yasniy</i>	
Simulation of High-frequency Induction Heating.....	39
<i>Dmytro Sorokin</i>	
A Simulation Methodology for Circular Economy Implementation.....	43
<i>Edna Guevara-Rivera, Roberto Osorno-Hinojosa and Victor-Hugo Zaldivar-Carrillo</i>	
Estimation of the Durability of Technological Rotating Objects by Data on the Displacement of Their Surface Points	49
<i>Galyna Grygorchuk, Andriy Oliylyk, Lyubomyr Grygorchuk, Vitaliy Rys and Volodymyr Tyrlych</i>	
Comparative Effectiveness of Some Approaches to Extracting Most Informative Factors Influencing Algae Bioproductivity	53
<i>Halyna Pidnebesna and Volodymyr Stepashko</i>	
Information Technologies for Process Analysis during Flight	57
<i>Hanna Polozhevets, Dariia Ovcharenko and Yurii Vitruck</i>	
High-performance Modeling Methods of Feedback-nanoporous Cyber Systems using Nonlinear Adsorption Equilibrium of Gas Cleaning	61
<i>Igor Boyko, Mykhaylo Petryk, Maria Petryk and Ivan Mudryk</i>	
Analysis of Deterministic Components of Biperiodically Correlated Random Signals	65
<i>Ihor Javorskyj, Roman Yuzefovych, Oksana Dzeryn and Mykola Varyvoda</i>	
Numerical Simulation to Control the Spread of Pollutants in Areas with Complex Surface.....	69
<i>Irina Vergunova, Viktor Vergunov and Iuliia Rosemann</i>	
Simulation and Analysis of Information Dissemination in Vehicular Ad-Hoc Networks.....	73
<i>Jiri Jelinek</i>	

The Use of Data Mining Techniques for Analysis of Menstrual Cycle Parameters and Prognosis of Migraine Symptoms in Reproductive Age Women	77
<i>Larysa Malanchuk, Mariia Riabokon, Artem Malanchuk, Serhiy Malanchuk, Svitlana Riabokon and Olha Kovalchuk</i>	
Interval Evaluation of Stationary State Probabilities for Markov Set-Chain Models.....	82
<i>Leonid Lyubchyk, Galyna Grinberg, Maria Lubchick, Alexey Galuza and Olena Akhiezer</i>	
Sports Areas: Optimization of Lighting Devices Placement.....	86
<i>Lesia Buiak, Andriy Mushak, Nadiya Khoma, Svitlana Khoma-Mohylska and Larysa Khokhlova</i>	
Information System Of Ecological Monitoring “Bioindicator - Forest Marten”.....	90
<i>Mariia Talakh, Serhii Golub and Viacheslav Hantyyuk</i>	
Conditional Entropy of DNA	94
<i>Marta Vohnoutová, Libor Dostálek, Iva Dostálková and Lenka Gahurová</i>	
Automatic Aircraft Collisions Algorithm Development for Civil Aircraft	98
<i>Mihaela Luminita Costea, Cătălin Nae, Nicolae Apostolescu, Florin Costache, Irina-Carmen Andrei, Gabriela-Liliana Stroe and Augustin Semenescu</i>	
Synthesis of Plane Rectangular Array with Taking into Account the Mutual Influence of Radiators.....	104
<i>Mykhaylo Andriychuk</i>	
Port Tariffs Discounting Mechanism Optimization	108
<i>Mykhaylo Voynarenko and Anatoliy Kholodenko</i>	
Identification the Model of Electric Power Generation by Small Hydroelectric Power Station Based on Artificial Bee Colony Algorithm	113
<i>Mykola Dyvak, Iryna Oliinyk, Mykhailo Sopiha, Viktor Sopiha and Yuriy Franko</i>	
Mathematical Model of Dynamics of Generated Electric Power by Photovoltaic Installation Taking into Account a Seasonality Factor	117
<i>Mykola Dyvak, Krzysztof Górecki, Janusz Zarębski, Natalia Porplytsya, Jacek Dąbrowski and Ewa Krac</i>	
Artificial Bee Colony Algorithm with Modified Operators of Determining the Profitable Food Sources for Identification the Models of Atmospheric Pollution by Nitrogen Dioxide.....	122
<i>Mykola Dyvak, Natalia Porplytsya, Andriy Pukas, Iryna Voytyuk, Nazar Huliiev, Vitaliy Pryvrotskyy</i>	
Synthesis of Ukraine Budget Revenues Model in Conditions of Shadow Economy using Modified Method of Structural Identification	126
<i>Mykola Dyvak, Natalia Porplytsya, Irena Pidhurska, Vasyl Brych, Liliana Horal and Nataliya Halysch</i>	
Parameters Identification Method of Interval Discrete Dynamic Models of Air Pollution Based on Artificial Bee Colony Algorithm.....	130
<i>Mykola Dyvak</i>	
Modeling of the Temperature Regime of the District Heating System in the Context of Energy Efficiency and Reduction of Environmental Impact	136
<i>Mykola Gavrylenko, Mykhailo Fedirko, Nataliia Dziubanovska, Halyna Pyrih, Vasyl Brych, and Nataliya Halysch</i>	
Modeling of the Estimation of the Time to Failure of the Information System for Critical Use....	140
<i>Oleg Bisikalo, Viacheslav Kovtun and Oksana Kovtun</i>	
General Method for Constructing of the Exact Solution of the Problem for Non-Stationary Heat Conductivity Equation in the Complex Field	144
<i>Oleg M. Lytvyn, Galina Zalyzhna, Inna Nefodova, Iuliia Pershyna and Olesia Nechuiviter</i>	

Explicit Formulas for Calculating Fourier Coefficients of Three Variables Using Tomograms ...	148
<i>Oleg M. Lytvyn, Oleksandra Lytvyn and Oleg O. Lytvyn</i>	
Method of Gas Consumption Change-point Detection Based on Seasonally Multicomponent Model	152
<i>Oleg Nazarevych, Yuriy Leshchyshyn, Serhii Lupenko, Volodymyr Gotovych, Grigorii Shymchuk and Nataliya Shablii</i>	
Mathematical Spatial Minerals Distributing Model by Interlineation Methods of Matrix-functions	156
<i>Oleg O. Lytvyn, Oleg M. Lytvyn, Olena Chorna and Hennadii Kaniuk</i>	
Method of Statistical Data Processing for Two-Stage Fatigue Tests.....	160
<i>Olena Kozhokhina, Svyatoslav Yutskevych, Oleksandr Radchenko, Viktor Gribov and Oleksii Chuzha</i>	
Forecasting Regional Migration Flows	165
<i>Olena Ovchynnikova, Olena Nahornova, Inna Mylko, Svitlana Begun, Nadiia Buniak and Nataliia Kolenda</i>	
Mathematical Methods for Optimizing Big Data Processing	170
<i>Olena Syrotkina, Mykhailo Aleksieiev, Borys Moroz, Serhii Matsiuk, Olga Shevtsova and Andrii Kozlovskiy</i>	
Mathematical Methods for Detecting and Localizing Failures in Complex Hardware/Software Systems.....	177
<i>Olena Syrotkina, Oleksandr Aziukovskiy, Iryna Udovyk, Oleksii Aleksieiev, Serhii Prykhodchenko and Leonid Ilyin</i>	
Assessing the Investment Capacity of the Agricultural Sector: Case of Ukraine.....	183
<i>Pavlo Hryhoruk, Nila Khrushch and Svitlana Grygoruk</i>	
Modeling the Influence of Diffusion Effects on Carbon Monoxide Catalitic Oxidation	188
<i>Petro Kostrobij and Iryna Ryzha</i>	
Using the Computational Fluid Dynamic Software to Mixing Process Modeling in The Industrial Scale Vessel with Side-Mounted Agitator	192
<i>Roman Havryliv, Iryna Kostiv and Volodymyr Maystryk</i>	
Multi-Channel Chaotic System.....	196
<i>Roman Voliansky, Vitaliy Kuznetsov, Nina Volianska, Oleg Klyuyev and Iurii Shramko</i>	
Calculation and Behavior of Lyapunov's Exponents for Incommensurate Superstructure Described by Two-Components Parameter of Order.....	200
<i>Sergiy Sveleba, Ivan Katerynychuk, Ivan Karpa, Ivan Kunyo, Volodymyr Rak and Oleksandr Yashchuk</i>	
Comparative Analysis of Existing Cardiac Output Measurement Methods.....	204
<i>Serhii Levytskii and Kostiantyn Shevchenko</i>	
Method of Statistical Processing of Discrete Cycle Random Processes, by their Reduction to Isomorphic Periodic Random Sequences.....	209
<i>Serhii Lupenko, Iaroslav Lytvynenko Stadnyk and Nataliia</i>	
Mathematical Modeling of Non-stationary Processes During Train Movement	213
<i>Serhiy Buryakovskiy, Artem Maslii, Danylo Pomazan and Andrii Maslii</i>	
Fast Reconstruction Algorithm for Contactless Inductive Flow Tomography	217
<i>Thomas Wondrak, Ralf T. Jacobs and Peter Faber</i>	
Method of Probability Distribution Fitting for Statistical Data with Small Sample Size	221
<i>Valeriyi Kuzmin, Maksym Zaliskiy, Roman Odarchenko, Oksana Polishchuk, Olga Ivanets and Olga Shcherbyna</i>	

Analysis of the Development of Socio-Cultural Potential of Ukraine with the Application of the Apparatus of Fuzzy Logic	225
<i>Vasyl Pryimak and Andrii Hrytsaiko</i>	
Formal Outlines of Case-Based Modelling of Data and Knowledge Sources for Drilling Control	231
<i>Vasyl Sheketa, Iurii Shcherbiak, Volodymyr Pikh, Yulia Romanyshyn, Mykola Chesanovskyy and Miroslav Kopnický</i>	
Methods Mathematical Models of the Process of Filtration of Substances in Complex Porous Structures.....	235
<i>Yaroslav Pyanylo</i>	
Features of Artificial Bee Colony Based Algorithm Realization for Parametric Identification Method of the Interval Discrete Dynamic Models	239
<i>Yevhen Kedrin, Mykola Dyvak, Andriy Pukas, Iryna Voytyuk, Yurii Maslyiak and Oleksandr Papa</i>	
Multiple-choice Classification of Radio Navigation Systems Technical State.....	246
<i>Oleksii Zuiev, Oleksandr Solomentsev and Yuliia Petrova</i>	

SECTION 2 Specialized Computer Systems

Queuing Model of Distance Measuring Equipment for Capacity Estimation	250
<i>Anastasiia Turovska and Ivan Ostroumov</i>	
Remote Synthesis of Computer Devices for FPGA-Based IoT Nodes.....	254
<i>Anatoliy Melnyk and Viktor Melnyk</i>	
Development of Theory, Scope and Tools for Entropy Signals and Data Processing	260
<i>Artur Voronych, Lyubov Nykolaychuk, Taras Grynychshyn, Volodymyr Hryha, Stepan Melnychuk and Yaroslav Nykolaychuk</i>	
High-performance Analyzing Methods for Tremor-objects Abnormal States of Neuro-biosystems with Cognitive Feedbacks.....	265
<i>Ivan Mudryk, Dmytro Mykhalyk and Mykhaylo Petryk</i>	
Estimation the Risk of Airplane Separation Lost by Statistical Data Processing of Lateral Deviations.....	269
<i>Ivan Tsymbaliuk, Oleg Ivashchuk and Ivan Ostroumov</i>	
Optimization of Distributed Phase Shift Beamforming Configuration by using Convex Hull	273
<i>Jan Kubr, Viktor Černý and Alexandru Mihnea Moucha</i>	
Cooperative Universal Risk Warning Systems in Motorised Individual Traffic – Using the Example of Collisions with Wildlife	278
<i>Kevin Seipel, Eva Weidemann, Eduard Hepner and Robert Hoyer</i>	
Fuzzy Logic Application in Automation Control.....	282
<i>Linos Nchena</i>	
Concept for the Large Scale Deployment of Ambient Assisted Living Systems	288
<i>Ludwig Schiller, Manuela Wuehr, Rainer Poeschl and Wolfgang Dorner</i>	
Multisensor UAV System for the Forest Monitoring	293
<i>Milan Novák, Miloš Prokyšek, Petr Doležal, Martin Hais, Stanislav Grill, Markéta Davidková, Jakub Geyer, Peter Hofmann and Rajan Paudyal</i>	

Information Technology for Recurrent Laryngeal Nerve Identification with Adaptive Adjustment of the Electrophysiological Method	297
<i>Mykola Dyvak, Andriy Dyvak, Dmytro Osadchuk, Volodymyr Tymets, Viktor Shidlovsky and Larysa Kovalska</i>	
Fuzzy Model of the IT Project Environment Impact on its Completion	302
<i>Nadiia Vasylykiv, Iryna Turchenko and Lesia Dubchak</i>	
Generators of Some Kinds Random Erlang Numbers and Estimation of Their Complexity	306
<i>Petro Pekh, Olena Kuzmych, Nataliia Bahniuk, Nina Zdolbitska and Iaroslav Pasternak</i>	
Air Quality Monitoring System: Towards IoT based system for Air Pollutant Concentration Prediction	311
<i>Rasha Shakir AbdulWahhab</i>	
Structure and Functioning of Information Systems of Background Monitoring of Landscape Elements of Gorgany Nature Reserve	317
<i>Yaroslav Nykolaychuk, Yaroslav Petrashchuk, Olena Slobodian, Ihor Pitukh, Taras Grynychyshyn, Lyubov Nykolaychuk and Volodymyr Hryha</i>	
Structures and Characteristics of High-performance Multi-bit Streaming Multiplayers.....	323
<i>Yaroslav Nykolaychuk, Alina Davletova, Petro Humennyi, Nataliia Vozna, Ihor Pitukh and Oleg Zastavnyy</i>	
Theoretical Principles for Determining Correlation Entropy, Structure and System Characteristics of Special-Purpose Processors.....	327
<i>Yaroslav Nykolaychuk, Nataliia Vozna, Andriy Segin, Ihor Pitukh, Taras Pastukh and Ivan Albanskiy</i>	
Structures and Multifunctional Characteristics of Parallel ADCs used in Cyber-Physical Systems.....	333
<i>Yaroslav Nykolaychuk, Nataliia Vozna, Oleg Zastavnyy, Ihor Pitukh, Petro Humennyi and Ivan Albanskiy</i>	
Information Technology of Motor Vehicle Databases Use to Prevent Terrorist Emergencies	339
<i>Yuliia Honcharenko, Natalia Kasatkina, Yurii Maslyiak, Bogdan Maslyiak and Lyudmyla Honchar</i>	

SECTION 3

Artificial Intelligence and Machine Learning

Modeling and Synthesis of Monochrome Interference Patterns of Flat Optical Surfaces With Typical Defects for Automatic Surface Quality Control.....	344
<i>Alexey Galuza, Maryna Shkoda, Olga Tevyasheva, Alla Belyaeva, Alla Savchenko and Ivan Kolenov</i>	
A Light-weight Method to Foster the (Grad)CAM Interpretability and Explainability of Classification Networks	348
<i>Alfred Schöttl</i>	
Evolving Neo-Fuzzy System for Distorted Data Online Processing	352
<i>Alina Shafronenko, Yevgeniy Bodyanskiy, Iryna Pliss and Sergiy Popov</i>	
Trust in the European Central Bank: Using Data Science and predictive Machine Learning Algorithms	356
<i>Andrii Skirka, Bogdan Adamyk, Oksana Adamyk and Mariana Valytska</i>	
Predictive Analytics to Improve Road Safety.....	362
<i>Benedikt Gräler, Imke Ines Klatt, Martin Pontius and Albert Remke</i>	

Predicting the Risk of Deer-vehicle Collisions by Inferring Rules Learnt from Deer Experience and Movement Patterns in the Vicinity of Roads.....	368
<i>Christian von Hoermann, Raphaela Pagany, Katrin Kirchner, Wolfgang Dorner, Marco Heurich and Ilse Storch</i>	
Wind Turbine Yaw Angle Control using Artificial Neural Networks	374
<i>David Esteban Albadan Molano and Diego Alejandro Barragan Vargas</i>	
Genetic Algorithm for Solution of the Problem of Optimal Location of the Distributed Electrical Networks	380
<i>Dmytro Goncharenko, Andrii Oliinyk, Ievgen Fedorchenko, Serhii Korniienko, Alexander Stepanenko, Anastasia Kharchenko and Yuliia Fedorchenko</i>	
Increasing the Classification Accuracy of EEG based Brain-computer Interface Signals	386
<i>George Dimitrov, Pavel Petrov, Inna Dimitrova, Galina Panayotova, Ivan Garvanov, Oleksii Bychkov, Eugenia Kovatcheva and Pepa Petrova</i>	
Fault Prediction of Wind Turbine Gearbox Based on SCADA Data and Machine Learning	391
<i>Haroon Rashid, Erfan Khalaji, Jawad Rasheed and Canras Batunlu</i>	
Forecasting of Wind Turbine Output Power Using Machine learning.....	396
<i>Haroon Rashid, Waqar Haider and Canras Batunlu</i>	
6-DOF Grasp Detection for Unknown Objects	400
<i>Henry Schaub and Alfred Schöttl</i>	
High-Accuracy Particulate Matter Prediction Model Based on Artificial Neural Network.....	404
<i>Jelena Misic and Vera Markovic</i>	
Analysis of the Effectiveness of an Investment Project Using Statistical Bayesian Networks.....	408
<i>Mariia Voronenko, Oleksandr Naumov, Larisa Naumova, Elzara Topalova, Viktoriia Filippova and Volodymyr Lytvynenko</i>	
Requirements for Prescriptive Recommender Systems Extending the Lifetime of EV Batteries..	412
<i>Markus Eider and Andreas Berl</i>	
Promising new Techniques for Computer Network Traffic Classification: A Survey.....	418
<i>Michal Konopa, Jan Fesl and Jan Jancek</i>	
The Applying Processing Intelligence Methods for Classify Persons in Identify Personalized Medication Decisions	422
<i>Nataliia Melnykova, Nataliya Shakhovska, Volodymyr Melnykov, Mariana Zakharchuk, Mykola Logoyda and Vitalii Mahlovanyi</i>	
A Deep Learning Algorithm for Solving the Cubic Schrödinger Equation	426
<i>Nevena Dugandžija</i>	
Gesture Detection in Digital Image Processing based on the Use of Convolutional Neuronal Networks	430
<i>Pawel Golec, Wieslawa Gryncewicz, Krzysztof Hauke, Marcin Hernes and Artur Rot</i>	
Risk Prediction of Wildlife-vehicle Collisions Comparing Machine Learning Methods and Data Use	436
<i>Raphaela Pagany, Javier Valdes and Wolfgang Dorner</i>	
Open Source Speech Recognition on Edge Devices	441
<i>René Peinl, Basem Rizk and Robert Szabad</i>	
Adaptive Mechanisms for Parallelization of the Genetic Method of Neural Network Synthesis...	446
<i>Serhii Leoshchenko, Andrii Oliinyk and Sergey Subbotin</i>	

Towards Classifying Parts of German Legal Writing Styles in German Legal Judgments	451
<i>Stefanie Urchs, Jelena Mitrović and Michael Granitzer</i>	
Forecasting Financial Time Series Using Combined ARIMA-ANN Algorithm.....	455
<i>Vasyl Hryhorkiv, Lesia Buiak, Andrii Verstiak, Mariia Hryhorkiv, Oksana Verstiak and Kateryna Tokarieva</i>	
The Construction of Formal Approaches for Errors Interpretation in Intellectual Systems.....	459
<i>Vasyl Sheketa, Roman Vovk, Mariana Bihun-Chesanovska, Volodymyr Pikh, Yulia Romanyshyn and Mykola Pasyeka</i>	
Evolving Fuzzy-Probabilistic Neural Network and Its Online Learning	465
<i>Yevgeniy Bodyanskiy, Anastasiia Deineko, Iryna Pliss and Olha Chala</i>	

SECTION 4 Software Engineering

A Case Study Validation of the Pair-estimation Technique in Effort Estimation of Mobile App Development Using Agile Processes	469
<i>Abdullah Altaleb, Hussain Alhashimi and Andy Gravell</i>	
Development of a web-based Process Monitoring System for an Aluminium Die-Casting Company and Experiences in the Production Environment	474
<i>Fabian Mielke and Wolfgang Schlüter</i>	
Subsystem Inheritance and Composition in Complex Systems	478
<i>Ioan Crisan</i>	
A Software Architecture for Video Analytics.....	483
<i>Ivan Cabezas and Julian Palacios</i>	
Formalization of Scientific Researches Results in Corporate Knowledge Bases As a Tool of Their Accumulation.....	488
<i>Mykhailo Susla, Roman Pasichnyk, Andriy Melnyk, Natalia Pasichnyk, Olena Vasylykiv and Olexander Androshchuk</i>	
Mathematical Modeling of the Estimation Process of Functioning Efficiency Level of Information Web-Resources	492
<i>Mykola Dyvak, Andriy Melnyk, Andrii Kovbasistyi, Ruslan Shevchuk, Oksana Huhul and Vasyl Tymchyshyn</i>	
Sequent Calculus for a Program-oriented Predicate Logic over Complex-Named Data.....	497
<i>Mykola Nikitchenko, Oksana Shkilniak and Stepan Shkilniak</i>	
Method of Robotic Process Automation in Software Testing Using Artificial Intelligence.....	501
<i>Nataliya Yatskiv, Solomiya Yatskiv and Anatoliy Vasylyk</i>	
Relations of Logical Consequence in Program-oriented Logics of Quasiary Predicates	505
<i>Oksana Shkilniak</i>	
3D Mapping to Collect Volunteered Geographic Information	509
<i>Sebastian Wöllmann, Roland Zink and Melanie Piser</i>	
Categorisation of Computational Methods for the Extraction and Analysis of Vehicle Trajectory Data leading to an Increase in Road Safety	514
<i>Serge Lamberty, Eszter Kalló, Moritz Berghaus, Adrian Fazekas and Markus Oeser</i>	

Execution Frequency and Energy Optimization for DVFS-enabled, Near-threshold Processors .518	
<i>Sofia Mäkikyrö, Samuli Tuoriniemi, Risto Anttila and Lauri Koskinen</i>	
Reduction of Server Load by Means of CMS Drupal 523	
<i>Viktor Satsyk, Roman Grudetsky, Olena Kuzmych, Nataliia Bahniuk, Liudmyla Hlynchuk and Yulia Melnychuk</i>	
Multi-Agent Software Architecture for Distributed Virtual Reality Systems 529	
<i>Volodymyr Duchenchuk and Volodymyr Boublik</i>	

SECTION 5

Information in Economic Activity and Digital Business Modeling

Fiscal Aspects of the Functioning of the Electronic Declaration System of Citizens' Income and Property in Ukraine 533	
<i>Andrii Krysovatyi, Volodymyr Valihura, Inna Hutsul, Fedir Tkachyk and Volodymyr Dmytriv</i>	
Optimal Price Choice through Buyers' Preferences Entropy 537	
<i>Andriy Goncharenko</i>	
The Ant Colony Probabilistic Model Equivalency to the Options Uncertainty Extremized One .. 541	
<i>Andriy Goncharenko</i>	
The Level of Fiscal Decentralization in Ukraine: Modeling of Indicative Parameters 545	
<i>Oleh Vatslavskyi and Anna Ivanova</i>	
The Global Trade Competition: Challenge for Ukraine 549	
<i>Antonina Farion-Melnyk, Lesia Marushchak, Olha Pavlykivska, Nadiia Moskaliuk, Mykhailyna Farion and Tetiana Slipchenko</i>	
Challenges for Knowledge Management in Digital Business Models 555	
<i>Artur Rot and Malgorzata Sobinska</i>	
Robotic Process Automation: An Overview and Comparison to Other Technology in Industry 4.0 559	
<i>Bernhard Axmann and Harmoko Harmoko</i>	
Structural Change in Labor Market Influenced by Artificial Intelligence: Theoretical and Empirical Analysis 563	
<i>Daryna Rozum, Nadiya Grazhevska and Volodymyr Virchenko</i>	
Development of Elements of ERP-system of Association of Co-owners of Multi-apartment Buildings 567	
<i>Dmytro Brechko, Nataliia Maksyshko and Sergey Ivanov</i>	
Identification of Stakeholders Importance for the Company's Social Responsibility using the Analytic Hierarchy Process 573	
<i>Ihor Oleksiv, Halyna Lema, Viktoriya Kharchuk, Taras Lisovych, Oleksandr Dluhopolskyi and Tetiana Dluhopolska</i>	
Mathematical Model for Prediction the Dynamics of Organic Traffic at E-commerce Web-site in the Process of its Search Engine Optimization 577	
<i>Iryna Madiudia, Natalia Porplytsya and Maryna Nagara</i>	
Accounting and Financial Reporting System in the Digital Economy 581	
<i>Iryna Spilnyk, Ruslan Brukhanskyi and Olexiy Yaroshchuk</i>	

Models of Rental Payments Formation for Agricultural Land Plots Taking into Account the Ecological Level of Economy	585
<i>Lesia Buiak, Oksana Bashutska, Kateryna Pryshliak, Vasyl Hryhorkiv, Mariia Hryhorkiv and Vitaliy Kobets</i>	
Polyglot Persistence in Conceptual Modeling for Information Analysis.....	590
<i>Matthias Kolonko and Sabine Müllenbach</i>	
Specificity of Corporate Culture Modeling at Industrial Enterprises in Conditions of Digital Business Transformation.....	595
<i>Mykhailo Vedernikov, Inna Sandyga, Lesia Volianska-Savchuk, Oksana Chernushkina, Maria Zelena and Olena Koshonko</i>	
Modeling of Controlling Activity as an Instrument of Influence on Motivation in the Personnel Management System of Industrial Enterprises.....	601
<i>Mykhaylo Voynarenko, Mykhailo Vedernikov, Lesia Volianska-Savchuk, Maria Zelena, Natalia Bazaliyska and Olga Baksalova</i>	
Modeling Emergence Properties of Economic System	607
<i>Mykhaylo Voynarenko, Larysa Lazebnyk, Viktoriya Hurochkina, Olena Kovalenko and Olena Menchynska</i>	
Intellectualization of the IT Sector Enterprise Management Process in the Context of Ensuring Economic Security: Pedagogical Aspects.....	613
<i>Myroslav Kryshchanovych, Svitlana Kryshchanovych, Yuriy Kozlovskiy, Nataliya Mukan and Olena Kvas</i>	
Modeling Seller Behavior in the Ukrainian Computer Market	617
<i>Nataliya Melnyk, Mykola Dyvak, Bohdan Melnyk, Petro Stakhiv, Ivan Dyyak and Rostyslav Mykhailyshyn</i>	
Modelling the Level of Energy Security at Enterprises in the Context of Environmentalization of Their Innovative Development	621
<i>Oksana Mykoliuk, Valentyna Bobrovnyk, Valentyna Fostolovych, Nataliia Prylepa and Hanna Kucherova</i>	
Organizational Network Analysis as a Tool for Leadership Assessment in Software Development Team.....	626
<i>Oksana Zhylynska, Anton Chornyi, Volodymyr Dzhuliy and Liudmyla Yemchuk</i>	
Control and Accounting of the Transportation Services Self-cost using GPS	631
<i>Oleg Shevchuk, Mykhailo Bryk, Oksana Desyatnyuk, Vasyl Voitseshyn and Volodymyr Muravskiy</i>	
Semantic Core Building of a Site Based on Clustering Algorithms	635
<i>Oleh Adamiv, Svitlana Adamiv, Vasyl Koval, Ivanna Andriychuk and Viktor Ostroverkhov</i>	
The Methodology of Hierarchical Ordering of Threats to Economic Security as the Basis for Educational and Practical Application for the Management of IT Sphere Enterprises.....	639
<i>Oleksandr Sylkin, Myroslav Kryshchanovych, Petro Petrovskiy, Myroslava Sirant and Nataliya Stetsyuk</i>	
Fractionally Cointegrated Vector Autoregression Model of Spread Estimation for Metals.....	643
<i>Olena Liashenko, Tetyana Kravets and Olha Bobro</i>	
Marketing Provision Of Realization Of Entrepreneurship Potential As The Basis Of Enterprise's Competitiveness.....	647
<i>Olga Gonchar, Iryna Polishchuk, Valentyna Khachatryan, Olha Ostapchuk, Andrii Bitiy and Irina Gvozdecka</i>	

Construction of Economic Models of Ensuring Ukraine's Energy Resources Economy	651
<i>Olga Kneysler, Uliana Andrusiv, Nataliia Spasiv, Liliya Marynychak and Olha Kryvytska</i>	
The Macroeconomic Model of Modern Global Terrorism	657
<i>Olha Kovalchuk and Mykola Shynkaryk</i>	
Estimating the Competitiveness Level of Enterprises Based on the Functional Effectiveness Model.....	662
<i>Serhii Spivak, Iryna Spivak and Svitlana Krepych</i>	
Analytical Model of Deposit Portfolio Optimization in Ukrainian Banks.....	666
<i>Svitlana Luchyk, Vasil Luchyk, Marharyta Luchyk, Yulia Manachynska, Volodymyr Yevdoshchak and Konon Bagrii</i>	
Estimating the Efficiency of the Energy Service Market Functioning in Ukraine	670
<i>Vasyl Brych, Volodymyr Manzhula, Bogdan Brych, Nataliya Halys, Yuliia Ursakii and Viktoriia Homotiuk</i>	
Strategy of Effective Pricing Policy of Biofuel Enterprises.....	674
<i>Vasyl Brych, Volodymyr Manzhula, Nataliya Halys, Ganna Zhekalo, Galyna Liakhovych and Oksana Vakun</i>	
Communication Model of Energy Service Market Participants in the Context of Cyclic Management City Infrastructure	678
<i>Vasyl Brych, Volodymyr Manzhula, Olena Borysiak, Galyna Liakhovych, Nataliya Halys and Vitaliy Tolubyak</i>	
A Fuzzy Assessment of the Development of the National Labor Market of Ukraine.....	682
<i>Vasyl Pryimak, Bohdan Melnyk, Olga Holubnyk, Tetyana Kostyshyna and Vasyl Brych</i>	
Expediency of Reducing and Cancellation of Customs Duty's Level on Exports in Ukraine and in the World	687
<i>Vasyl Voitseshyn, Oksana Desyatnyuk and Oleg Shevchuk</i>	
Practical-oriented Education in Modeling and Simulation for Cyber-Physical Systems	691
<i>Volodymyr Kazymyr, Serhiy Shkarlet and Anatolijs Zabašta</i>	
The Fiscal Policy Impact on Indicators of the State's Economic Growth	695
<i>Volodymyr Martyniuk, Oleksandr Dluhopolskyi, Sviatoslav Kniaz, Nazar Podolchak, Yuliia Muravska and Bogdana Martyniuk</i>	
Investment Attractiveness of Land Resources of Ukraine	699
<i>Volodymyr Shvets, Liubov Shevtsiv, Nataliia Mishchuk, Bohdan Melnyk, Yuriy Humen and Marija Mudrak</i>	
A Technique for Integral Evaluation and Forecast of the Performance of a Complex Economic System	704
<i>Volodymyr Stepashko, Roman Voloschuk and Serhiy Yefimenko</i>	
Theoretical and Empirical Analysis of the Relationship Between Monetary Policy and Stock Market Indices.....	708
<i>Yevgenii Sova and Iryna Lukianenko</i>	
Economic and Mathematical Modeling in Informational Support of Innovational Processes Management Functions	712
<i>Zakharii Varnalii, Mykhaylo Voynarenko, Liudmyla Yemchuk, Larysa Dzhulii, Larysa Skorobohata and Lesya Bushowska</i>	

Analysis of the Implementation Efficiency of the new Computer-communication Form of Accounting	718
<i>Zenovii-Mykhailo Zadorozhnyi and Volodymyr Muravskiy</i>	
Investigation of Information Sharing Behavior in Work Teams	722
<i>Zora Řihová</i>	

SECTION 6

Smart Grids and Intelligent Consumers

Motivation of the Smart Energy: Fabrication Industries as a Case Study.....	726
<i>Haroon Rashid, Muhammad Saleh Rashid and Canras Batunlu</i>	
Use and Programmatic Extension of PowerFactory for the Implementation of Automated Network Planning at the Distribution Grid Level	731
<i>Hermann Kraus and Oliver Brückl</i>	
Structure Prediction in Uncertain Temporal Networks.....	737
<i>Ladislav Beranek and Radim Remes</i>	
Mixed-Integer-Linear-Programming Model for the Charging Scheduling of Electric Vehicle Fleets	741
<i>Nicki Bodenschatz, Markus Eider and Andreas Berl</i>	

SECTION 7

Cyber Security and IT Law

A Behaviour based Ransomware Detection using Neural Network Models	747
<i>Eleni Ketzaki, Petros Toupas, Konstantinos Giannoutakis, Anastasios Drosou and Dimitrios Tzouvaras</i>	
Method for Determining Prime and Relatively Prime Numbers of $2n+k$ Type Based on the Periodicity Property.....	751
<i>Igor Yakymenko, Mykhailo Kasianchuk, Stepan Ivasiev, Ruslan Shevchuk, Yuriy Batko and Vladyslav Vasylykiv</i>	
The Monte Carlo Type Method of Attack on the RSA Cryptosystem.....	755
<i>Marek Wojtowicz, Dmytro Bodnar, Ruslan Shevchuk, Oksana Bodnar and Iryna Bilanyk</i>	
Respect for Information Rights of a Person as a Condition for Cybersecurity of Smart Cities Residents	759
<i>Mariia Pleskach, Oleh Zaiarnyi and Valentyna Pleskach</i>	
Cybersecurity: Technology vs Safety	765
<i>Olha Kovalchuk, Mykola Shynkaryk, Mariia Masonkova and Serhiy Banakh</i>	
Software for Automatic Estimating Security Settings of Social Media Accounts.....	769
<i>Ruslan Shevchuk, Andriy Melnyk, Oleh Opalko, Halyna Shevchuk</i>	
Don't Forget the User: From User Preferences to Personal Privacy Policies	774
<i>Stefan Becher, Armin Gerl and Bianca Meier</i>	
Algorithmic Support for Rabin Cryptosystem Implementation Based on Addition.....	779
<i>Stepan Ivasiev, Mykhailo Kasianchuk, Igor Yakymenko, Oksana Gomotiuk, Inna Shilynska and Lesia Bilovus</i>	

Cybercrime and Vulnerability of Ukrainian Critical Information Infrastructure	783
<i>Svitlana Mazepa, Libor Dostálek, Olga Sharmar and Serhiy Banakh</i>	
Cybercrime in Ukraine and the Cyber Security Game	787
<i>Svitlana Mazepa, Libor Dostálek, Vlastimil Křivan and Serhiy Banakh</i>	
Ways of Unauthorized Access to Medical Data and Approach to Organize Secure Access using Blockchain Technology	791
<i>Taras Maksymiv and Roman Chaplinskyi</i>	
Protected Distributed Data Storage Based on Residue Number System and Cloud Services	796
<i>Vasyl Yatskiv, Serhii Kulyna, Nataliya Yatskiv and Halyna Kulyna</i>	
Safe Decentralized Applications Development Using Blockchain Technologies.....	800
<i>Viktor Cheshun, Ihor Muliar, Vasyl Yatskiv, Ruslan Shevchuk, Serhii Kulyna and Taras Tsavolyk</i>	
Areas of Focus for Cloud Security Providers Assessment	806
<i>Vlasta Svatá and Martin Zbořil</i>	

SECTION 8

Image Processing

Perceptual Modelling of Unconstrained Road Traffic Scenarios with Deep Learning.....	811
<i>Jaswanth Nidamanuri, Anjali Poornima Karri and Hrishikesh Venkataraman</i>	
A Comparative Approach between Different Computer Vision Tools, Including Commercial and Open-source, for Improving Cultural Image Access and Analysis	815
<i>Jose Luis Preza Diaz, Amelie Dorn, Gerda Koch and Yalemisew Abgaz</i>	
Adaptive Immunohistochemical Image Pre-processing Method.....	820
<i>Oleh Berezsky, Oleh Pitsun, Bohdan Derish, Kateryna Berezska, Grygory Melnyk and Yuriy Batko</i>	
Method for Improving the Efficiency of Online communication Systems Based on Adaptive Multi-scale Transformation	824
<i>Olena Kolganova, Lidiia Tereshchenko, Alla Sitko, Viktoriia Kravchenko, Svitlana Kornienko, Viktoriia Volkogon, Zhanna Vasylieva-Shalamova, Mykola Shutko and Volodymyr Shutko</i>	
Automated Object Recognition System based on Convolutional Autoencoder	830
<i>Pylyp Prystavka, Olga Cholyshkina, Serge Dolgikh and Denys Karpenko</i>	
Improving the Accuracy of Pedestrian Detection in Partially Occluded or Obstructed Scenarios	834
<i>Redge Melroy Castelino, Gabriel Passos Moreira Pinheiro, Bruno Justino Garcia Praciano, Giovanni Almeida Santos, Lothar Weichenberger and Rafael Timóteo De Sousa Júnior</i>	
Method of Tile Visualization Technology with Sorting of Scene Fragments	839
<i>Sergey Vyatkin, Alexander Romanyuk, Oksana Romanyuk, Mykola Nechyporuk, Liudmyla Savytska and Nataliia Dobrovolska</i>	
Optimized Finite Element Method using Free-Form Volume Patches for Deformation of Three-Dimensional Objects	845
<i>Sergey Vyatkin, Alexander Romanyuk, Oksana Romanyuk, Mykola Nechyporuk, Roman Chekhmestruk and Pavlo Mykhaylov</i>	
Photorealistic Object Reconstruction Using Perturbation Functions and Features of Passive Stereo Projection	851
<i>Sergey Vyatkin, Alexander Romanyuk, Oksana Romanyuk, Mykola Nechyporuk, Tatiana Troyanovskaya and Olena Tsikhanovska</i>	

Deformation Methods of Functionally Defined Objects using Perturbation Functions	858
<i>Sergey Vyatkin, Alexander Romanyuk, Mykola Nechyporuk, Anatoliy Snigur, Pavlo Mykhaylov and Roman Chekhmestruk</i>	
Advisory Framework to Interconnect Distributed Water Bodies Targeting Agriculture Farms ..	863
<i>Sunil Js, Manasa Karanam, Raja Vara Prasad Yerra and Hrishikesh Venkataraman</i>	
Smart Goal Keeper Prototype using Computer Vision and Raspberry Pi.....	867
<i>Syed Umaid Ahmed, Hamza Ayaz, Hamza Khalid, Anas Ahmed, Mohammad Affan and Din Muhammad</i>	
A Lossless Image Compression Algorithm Based On Group Encoding.....	871
<i>Vasyl Koval, Vasyl Yatskiv, Igor Yakymenko and Diana Zahorodnia</i>	
The Robustness of the VSSD Watermarking Algorithm to UDFE Image Deformations	875
<i>Zoran Milivojevic, Bojan Prlincevic, Zoran Velickovic and Dejan Blagojevic</i>	
Resilience of MDCS Watermarking Algorithm in Wireless Network Environment.....	881
<i>Zoran Velickovic, Zoran Milivojevic and Dejan Blagojevic</i>	

SECTION 9

Information Technologies in Historical Science

ReConFort Open Database - Digitisation of Historical Documents Influencing the Constitutional Forming Process in Europe for Open Access	885
<i>Armin Gerl, Ulrike Müßig and Harald Kosch</i>	
Digitized Historical and Cultural Heritage Consolidation Technologies: From a Territorial Resource to a National Portal	891
<i>Halyna Lypak, Nataliia Kunanets, Volodymyr Pasichnyk and Nataliia Veretennikova</i>	
Current Digital Travel Guide of Peregrinus Silva Bohemica Project.....	897
<i>Martina Kepka Vichrová, Pavel Hájek, Michal Kepka, Laura Fiegler, Mariann Juha, Wolfgang Dorner and Radek Fiala</i>	
Prospects for the Use and Improvement of Information Search Systems as Part of Development of Historical Research	901
<i>Volodymyr Tereshchenko</i>	

The Monte Carlo Type Method of Attack on the RSA Cryptosystem

Marek Wojtowicz
Institute of Mathematics
Kazimierz Wielki University
in Bydgoszcz
 Bydgoszcz, Poland
 mwojt@ukw.edu.pl

Dmytro Bodnar
Department of Economic Cybernetics
and Informatics
Ternopil National Economic University
 Ternopil, Ukraine
 bodnar4755@ukr.net

Ruslan Shevchuk
Department of Computer Science
Ternopil National Economic University
 Ternopil, Ukraine
 rsh@tneu.edu.ua

Oksana Bodnar
Institute of Pedagogics and Psychology
Ternopil Volodymyr Hnatiuk
National Pedagogical University
 Ternopil, Ukraine
 bodnarotern@ukr.net

Iryna Bilanyk
Pidstryhach Institute for Applied Problems of Mechanics and
Mathematics NAS of Ukraine
 Lviv, Ukraine
 i.bilanyk@ukr.net

Abstract — The RSA cryptosystem is the most widely used cryptosystem, and its security is based on the difficulty of factorization of big integers.

We study the possibility of determination of the secret key of an RSA cryptosystem by means of the Monte Carlo method applied to the continued fraction method. We develop and extend similar techniques studied earlier by Wiener, de Weger, and others.

Keywords — RSA, Cryptanalysis, Continued fraction, Monte Carlo method.

I. INTRODUCTION

RSA is an asymmetric encryption algorithm which works with a public and private keys called a key pair [1]; see below.

Let p, q be two large prime numbers, $N := pq$ be the modulus of RSA, $\varphi(N) := (p-1)(q-1)$ be the Euler function of N , and let e, d be the public and private key pair, less than $\varphi(N)$ and relatively prime with $\varphi(N)$, with

$$ed \equiv 1 \pmod{\varphi(N)}. \quad (1)$$

Then the encryption function $E(M)$ of a message M (with $\gcd(M, N) = 1$) is of the form

$$E(M) \equiv M^e \pmod{N},$$

and the decryption function $D(S)$ of an encrypted message S is of the form

$$D(S) \equiv S^d \pmod{N}.$$

Then, by (1), we have $D(E(M)) \equiv M \pmod{N}$.

Nowadays, RSA seems to be extremely secure, yet at the cost of the width of the modulus N . It has survived over 20 years of scrutiny and is in widespread use throughout the world [2,3]. The standard attack on the RSA cryptosystem involves factorization of N . Then, by (1) and the form of D , every message written with the public key can be decrypted.

In 1990, Wiener [4] proposed another method of attack on RSA. He proved that if $d < \frac{1}{3}N^{1/4}$ then d is the denominator of a convergent of the continued fraction determining the representation of the number e/N . The method is based on the following property [5, Theorem 184]:

If A is a real number and P/Q is an irreducible fraction such that

$$\left| A - \frac{P}{Q} \right| < \frac{1}{2Q^2}, \quad (2)$$

then P/Q is one of convergents of the continued fraction representing A .

In 2002, de Weger [6] showed that Wiener's attack on RSA can be strongly improved: by replacing (in Wiener's method) the continued fraction expansion of e/N by

$$A := \frac{e}{N - 2\sqrt{N} + 1}, \quad (3)$$

the key d can be obtained if the following relation holds:

$$\delta < \frac{3}{4} - \beta, \quad (4)$$

where $\delta = \log_N d$ and $\beta = \log_N |p - q|$, i.e.,

$$d = N^\delta \text{ and } \Delta := |p - q| = N^\beta \text{ for } \beta \in \left[\frac{1}{4}, \frac{1}{2} \right];$$

in the case of Wiener's attack we have $\delta < \frac{1}{4}$.

From inequality (4) it follows that the difference $\Delta = N^\beta$ cannot be too small. For example, if $\Delta < N^{1/4}$ then the attack by means of de Weger's method allows us to determine efficiently the private key d , because then $d < \sqrt{N}$, thus $\delta < 1/2$, which significantly improves Wiener's result.

Hence the practical conclusion follows: when constructing a specific RSA system, it is necessary to choose prime numbers p, q , so that the number Δ is at least of the order of \sqrt{N} , and $d > N^{1/3}$.

Wiener's idea to attack on the RSA system by the method of continued fractions was developed in subsequent years among others by Blomer and May [7] (2004), Dujella [5] (2004), Nitaj [8] (2008), Maitra and Sarkar [9] (2008), and Chen, Hsueh, and Lin [10] (2009).

On page 20 of [6], de Weger suggests to consider the possibility of improving his results by including the numerical value of the public key e to the security analysis of the RSA system, i.e., examining the resistance of a given RSA system to a continued fraction attack with respect to the size of $\alpha := \log_N e$ (de Weger assumed that $\alpha \approx 1$, i.e., $e \approx N$).

The first research in this direction was carried out by Maitra and Sarkar [9]: they showed that if $q < p < 2q$, the RSA system is not secure (N can be factorized in $\text{poly}(\log N)$ time), when

$$d < \frac{1}{2}N^s \text{ and } ed^2 = O(N^{3/2-2s}), s < \frac{1}{2}.$$

By considering the convergents of the continued fraction expansion of the number

$$\frac{e}{N - \frac{3}{\sqrt{2}}\sqrt{N} + 1}, \quad (5)$$

Maitra and Sarkar obtained a generalization of inequality (4) with extra conditions on p, q .

In 2009, Chen, Hsueh, and Lin [10] applied the method of continued fractions to the number

$$\frac{e}{N - \frac{a+b}{\sqrt{ab}}\sqrt{N} + 1}, \text{ where } a, b > 0, \quad (6)$$

showing that the private key d can be determined if $\delta < \frac{3}{4} - \gamma$, where $\gamma = \log_N |ap - bq|$ (i.e., $|ap - bq| = N^\gamma$).

If $a = b = 1$, this method reduces to de Weger's attack (3), and to the Maitra-Sarkara method (5) for $a = 2b$.

The problem of factorization of large natural numbers, with applications to Mersenne numbers, was recently studied in the papers [11,12].

II. MAIN RESULT

Theorem 1. Let e, d be two positive integers $< \varphi(N)$ fulfilling relation (1):

$$ed = 1 + k\varphi(N) \text{ for some natural number } k,$$

where $N = pq$ and

$$q > p + 2\sqrt{p} + 1. \quad (7)$$

Then there exists a real number $c' \in [2, c_0]$, $c_0 = \sqrt{9/2}$, such that the following equality holds true:

$$\frac{e}{N - c'\sqrt{N} + 1} = \frac{k}{d}.$$

Proof. Let F be a function on $[2, c_0]$ of the form

$$F(c) = \frac{e}{N - c\sqrt{N} + 1} - \frac{k}{d}.$$

(Notice that $k < e$ because $d < \varphi(N)$, where $e\varphi(N) > ed = 1 + k\varphi(N) > k\varphi(N)$. Hence we should check only denominators d_j of the convergents k_j/d_j with numerators $k_j < e$, i.e., whether $2^{ed_j} \equiv 2 \pmod{N}$.)

We shall prove that

$$F(2) < 0 < F(c_0), \quad (8)$$

because then the result holds by the continuity of F .

Set $W = (N - c\sqrt{N} + 1) \cdot d$. Notice that $W > 0$ for $c \in [2, c_0]$. Then

$$\begin{aligned} W \cdot F(c) &= ed - k\varphi(N) - \\ &- k(N + 1 - c\sqrt{N} - N + (p + q) - 1) = \\ &1 - k(p + q - 2\sqrt{pq} - (c - 2) \cdot \sqrt{pq}). \end{aligned} \quad (9)$$

But since, by (7), $p + q - 2\sqrt{pq} > 1$, from (9) we obtain

$$W \cdot F(2) < 1 - k \leq 0,$$

which is the left hand side of (8).

Now, by (9),

$$W \cdot F(c_0) = 1 - k(q + p - c_0\sqrt{pq}).$$

Thus, $F(c_0) > 0$ if $q + p - c_0\sqrt{pq} \leq 0$, i.e.,

$$\sqrt{\frac{q}{p}} + \sqrt{\frac{p}{q}} \leq c_0.$$

The latter inequality is equivalent to

$$\frac{p}{q} + 2 + \frac{q}{p} \leq c_0^2 = \frac{9}{2},$$

thus, setting $x = p/q$, we obtain $x + x^{-1} - 2.5 \leq 0$, i.e., $x^2 - 2.5x + 1 = (x - 2) \cdot (x - 0.5) \leq 0$.

But since, by assumption, $x = p/q < 2$, the latter inequality holds true, which implies, by the above series of equivalences and implications, that $F(c_0) > 0$. This is the second required inequality in (8). The proof is complete.

Corollary. Let $c = \sqrt{5 - \frac{1}{r}}$, where $r \in [1, 2]$, thus $c \in [2, c_0]$. If the conditions of Theorem 1 are satisfied then there exists a rational number r , such that the private key d can be determined by a convergent of the continued fraction expansion of the number

$$w(c) := \frac{e}{N - c\sqrt{N} + 1}. \quad (10)$$

III. EXAMPLE

In practice, the corollary implies the effectiveness of the Monte Carlo method, which relies on a random selection of rational numbers $r_j, j=1,2,\dots$ from the interval $[1,2]$ and testing the congruence

$$2^{rd_j} \equiv 2 \pmod{N}$$

by means of denominators d_j of consecutive convergents of the continued fraction expansion of the numbers $w(c_j), j=1,2,\dots$, where c_j depends on r_j as in the Conclusion.

The numbers r_j can also be determined using the dyadic sequence:

$$1; 2; 1+\frac{1}{2}; 1+\frac{1}{2^2}, 1+\frac{3}{2^2}; 1+\frac{1}{2^3}, 1+\frac{3}{2^3}, 1+\frac{5}{2^3}, 1+\frac{7}{2^3}; \dots, (11)$$

or a sequence of fractions determined by consecutive primes p_k :

$$1; 2; 1+\frac{1}{2}; 1+\frac{1}{3}, 1+\frac{2}{3}; \dots; 1+\frac{1}{p_k}, 1+\frac{2}{p_k}, \dots, 1+\frac{p_k-1}{p_k}; \dots (12)$$

or a sequence of fractions $1+a/b$, where a, b are natural coprime numbers such that $a < b$:

$$1; 2; 1+\frac{1}{2}; 1+\frac{1}{3}, 1+\frac{2}{3}; 1+\frac{1}{4}, 1+\frac{3}{4}; 1+\frac{1}{5}, \dots, 1+\frac{4}{5}; \dots (13)$$

For example, for 9-digit prime numbers

$$p = 231961001, q = 371131003,$$

their product (modulus of an RSA) is a 17-digit number

$$N = qp = 86087918958014003,$$

and

$$\varphi(N) = (q-1)(p-1) = 86087918354922000.$$

In this example, we have $\delta = \beta = 1/2$, whence $\delta + \beta = 1 > 3/4$, so the necessary conditions (2) for de Weger's attack on the above RSA system are not satisfied.

We will now demonstrate the effectiveness of the Monte Carlo type attack described in the Corollary.

Testing the fractions of numbers $w(c)$ with the sequence of the form (11) we get that d is the denominator of the 11th convergent of the continued fraction expansion of number $w_1 = w(c) = w(\sqrt{1-r^{-1}})$ for

$$r = 1 + 304395/2^{20} = 1 + 304395/1048576:$$

$$\left[0; 1; \frac{108}{109}, \frac{217}{219}, \frac{8354}{8431}, \frac{8571}{8650}, \frac{291197}{293881}, \frac{590965}{596412}, \frac{22747867}{22957537}, \right.$$

$$\left. \frac{46086699}{46511486}, \frac{68834566}{69469023}, \frac{114921265}{115980509}, \frac{643440891}{649371568} \right].$$

By applying the sequence of the form (12) we can determine d for a lower denominator of the number $r-1$: k/d is the 10th convergent of the continued fraction expansion of $w_2 = w(c(1+30826/106189))$; of course, here the 6-digit number 106189 is prime:

$$\left[0; 1; \frac{108}{107}, \frac{217}{219}, \frac{8354}{8431}, \frac{8571}{8650}, \frac{291197}{293881}, \frac{590965}{596412}, \right.$$

$$\left. \frac{22747867}{22957537}, \frac{46086699}{46511486}, \frac{114921265}{115980509}, \frac{12342662054}{12456425949} \right].$$

The smallest denominator $r-1$ is obtained by testing the convergents of the continued fraction expansion of $w(c)$ by means of the sequence (13). The fraction k/d is the 10th convergent for $w_3 = w(c(1+1947/6707))$, and the 4-digit number 6707 is composite (here $6707 = 19 \cdot 353$):

$$\left[0; 1; \frac{108}{109}, \frac{217}{219}, \frac{8354}{8431}, \frac{8571}{8650}, \frac{291197}{293881}, \frac{590965}{596412}, \right.$$

$$\left. \frac{22747867}{22957537}, \frac{46086699}{46511486}, \frac{114921265}{115980509}, \frac{6136913744}{6193478463} \right].$$

Note that the first ten convergents of the continued fraction expansion of w_2 and w_3 are identical.

IV. SOME RECOMMENDATIONS FOR POSSIBLE USING THE CONTINUED FRACTIONS TOOLS IN CRYPTANALYSIS

Using a not widely spread properties of continued fractions we could improve the above algorithm or expand its possibilities. We build an expansion of a rational number by using the Euclidean algorithm. The representation is formed by subtracting away the integer part of a number and repeatedly inverting the remainder and subtracting away the integer part until the remainder is zero (for rational numbers). For irrational numbers this process is infinite. Furthermore, for algebraic irrationalities continued fractions are periodic.

Let a real number α have an expansion into a simple continued fraction

$$\alpha = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \dots}} = b_0 + \frac{1}{b_1} + \frac{1}{b_2 + \dots} = b_0 + \sum_{n=1}^{\infty} \frac{1}{b_n}, (14)$$

where b_0 is an integer, and b_k are positive integers.

In the algorithm described in the previous paragraph, we calculate the m th numerators A_m and m th denominators B_m of the m th approximant (convergent) of the continued fraction (14)

$$\frac{A_m}{B_m} = b_0 + \frac{1}{b_1} + \frac{1}{b_2 + \dots} + \frac{1}{b_m}.$$

But besides the convergents of continued fractions the best approximation we may obtain is by means of mediants. The mediant of two fractions a/b and c/d is defined as $(a+c)/(b+d)$. There we can apply the following mediants:

$$\frac{kA_m + A_{m-1}}{kB_m + B_{m-1}},$$

where $k = 1, 2, \dots, b_{m+1} - 1, m \geq 1$ if $b_{m+1} > 1$.

Let us consider how we can calculate the m th approximant of a continued fraction. There are a couple of

methods. It can be done by starting with b_m , and adding and inverting a proper fraction at each step back to b_0 . This is the algorithm “from bottom to top”.

Another way of calculating is “from top to bottom”. It is based on the Wallis-Euler recurrence relations [13-15]:

$$\begin{aligned} A_m &= b_m A_{m-1} + A_{m-2}, \quad m \geq 1, \\ B_m &= b_m B_{m-1} + B_{m-2}, \quad m \geq 1, \end{aligned} \quad (15)$$

where

$$A_{-1} = 1, A_0 = b_0, B_{-1} = 0, B_0 = 1.$$

Computation can be accelerated if we count only even or odd denominators of a continued fraction by means of the following formulas:

$$\begin{aligned} A_{2n+1} &= \left(1 + b_{2n} b_{2n+1} + \frac{b_{2n+1}}{b_{2n-1}}\right) A_{2n-1} - \frac{b_{2n+1}}{b_{2n-1}} A_{2n-3}, \quad n \geq 1, \\ B_{2n+1} &= \left(1 + b_{2n} b_{2n+1} + \frac{b_{2n+1}}{b_{2n-1}}\right) B_{2n-1} - \frac{b_{2n+1}}{b_{2n-1}} B_{2n-3}, \quad n \geq 1, \end{aligned}$$

with the initial conditions

$$A_1 = b_0 b_1 + 1, A_{-1} = 1, B_1 = b_1, B_{-1} = 0,$$

or

$$\begin{aligned} A_{2n+2} &= \left(1 + b_{2n+1} b_{2n+2} + \frac{b_{2n+2}}{b_{2n}}\right) A_{2n} - \frac{b_{2n+2}}{b_{2n}} A_{2n-2}, \quad n \geq 1 \\ B_{2n+2} &= \left(1 + b_{2n+1} b_{2n+2} + \frac{b_{2n+2}}{b_{2n}}\right) B_{2n} - \frac{b_{2n+2}}{b_{2n}} B_{2n-2}, \quad n \geq 1, \end{aligned}$$

with the initial conditions

$$A_0 = b_0, A_2 = b_0 b_1 b_2 + b_0 + b_2, B_0 = 1, B_2 = b_1 b_2 + 1.$$

Despite the fact that there are recurrent formulas for “from top to bottom” calculation, we can also apply other formulas that allow us to find the numerators and denominators of approximants immediately; in particular, the Euler-Minding formulas

$$\begin{aligned} A_m &= b_0 b_1 \dots b_m \left(1 + \sum_{k=0}^{m-1} \frac{1}{b_k b_{k+1}} + \sum_{k_1=0}^{m-3} \frac{1}{b_{k_1} b_{k_1+1} b_{k_2=k_1+2} b_{k_2+1}} + \dots + \sum_{k_1=0}^{m+1-2s} \frac{1}{b_{k_1} b_{k_1+1} b_{k_2=k_1+2} b_{k_2+1}} \dots \sum_{k_s=k_{s-1}+2}^{m-1} \frac{1}{b_{k_s} b_{k_s+1}}\right), \\ B_m &= b_1 b_2 \dots b_m \left(1 + \sum_{k=1}^{m-1} \frac{1}{b_k b_{k+1}} + \sum_{k_1=1}^{m-3} \frac{1}{b_{k_1} b_{k_1+1} b_{k_2=k_1+2} b_{k_2+1}} + \dots + \sum_{k_1=1}^{m+1-2r} \frac{1}{b_{k_1} b_{k_1+1} b_{k_2=k_1+2} b_{k_2+1}} \dots \sum_{k_r=k_{r-1}+2}^{m-1} \frac{1}{b_{k_r} b_{k_r+1}}\right) \end{aligned}$$

$$\text{where } s = \left\lfloor \frac{m+1}{2} \right\rfloor, r = \left\lfloor \frac{m}{2} \right\rfloor.$$

V. CONCLUSION

The RSA cryptosystem security problem is considered in the terms of vulnerability to a Monte Carlo attack.

By generalizing the de Weger attack method, using the continued fraction technique, the Monte Carlo method has been shown to be effective for decrypting the private key of a given RSA system.

In the attached example, we showed that our method can cover a much broader group of cases than the de Weger method. In addition, the same result was obtained with the help of three independent methods of selecting the rational parameter r from the interval (1.2), allowing to find such a value of the tested which allows us determining the private key.

More detailed results along with the appropriate software will be included in a separate article.

REFERENCES

- [1] R. L. Rivest, A. Shamir and L. M. Adleman, “A Method for Obtaining Digital Signature and Public-Key Cryptosystems” *Communications of ACM*, Vol. 21, No. 2, 1978, pp. 120-126. doi:10.1145/359340.359342.
- [2] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish,” *Procedia Computer Science*, vol. 78, pp. 617–624, 2016
- [3] Z. Hercigonja, D. Gimnazija, and C. Varazdin, “Comparative analysis of cryptographic algorithms and advanced cryptographic algorithms,” *International Journal of Digital Technology & Economy*, vol. 1, no. 2, pp. 1–8, 2016.
- [4] M. Wiener, “Cryptanalysis of short RSA secret exponents,” *IEEE Transactions on Information Theory*, Vol. 36, pp. 553–558, 1990.
- [5] A. Dujella, “Continued fractions and RSA with small secret exponent” *Tatra Mountains Mathematical Publications*, vol. 29, pp. 101–112, 2004.
- [6] B. De Weger, “Cryptanalysis of RSA with small prime difference” *Applicable Algebra in Engineering, Communication and Computing*, Vol 13 (1), pp. 17-28, 2002.
- [7] J. Blomer, A. May “A Generalized Wiener Attack on RSA, Public key cryptography” in *Proc. of 7th international workshop on theory and practice in public key cryptography*, Singapore, March 1–4, 2004. Proceedings. Bao, Feng (ed.) et al., Berlin: Springer. Lecture Notes in Computer Science 2947, 1–13 (2004).
- [8] A. Nitaj “Another generalization of Wiener’s attack on RSA” in *Vaudenay, S. (ed.) Africacrypt 2008. Lecture Notes in Computer Science*, Springer-Verlag Vol. 5023, pp. 174–190, 2008.
- [9] S. Maitra, S. Sarkar, Wu, Tzong-Chen (ed.) et al., “Revisiting Wiener’s attack – new weak keys in RSA” in *Proc. of 11th international conference, ISC 2008*, Taipei, Taiwan, 2008.
- [10] C.-Y. Chen, C.-C. Hsueh, Y.-F. Lin, “A Generalization of de Weger’s Method” in *Proc. of Fifth International Conference on Information Assurance and Security*, Xi’an, Taiwan, pp. 344-347
- [11] M. Kasianchuk, I. Yakymenko, S. Ivasiev et al. “The method of factorizing multi-digit numbers based on the operation of adding odd numbers” // *CEUR Workshop Proceedings, 8th International Conference Advanced Computer Information Technologies, ACIT 2018*; Ceske Budejovice, Czech Republic, June 2018. – P. 232-235.
- [12] S. Ivasiev, I. Yakymenko, M. Kasianchuk, R. Shevchuk et al. “Effective algorithms for finding the remainder of multi-digit numbers” in *Proc. of 2019 9th International Conference on the Advanced Computer Information Technologies (ACIT-2019)*, Ceske Budejovice, Czech Republic, June 2019, pp. 175–178.
- [13] H.S. Wall, “Analytic Theory of Continued Fractions”, *Reprinted by the American Mathematical Society*, Providence RI, 2000.
- [14] A. Cuyt, V. Brevik Petersen, B. Verdonk, H. Waadeland, W. B. Jones. *Handbook of Continued Fractions for Special Functions*, Dordrecht: Springer, 2008.
- [15] L. Lorentzen, H. Waadeland, “Continued fractions”, *Convergence theory, Amsterdam, Paris: Atlantis Press/Word Scientific*, Vol. 1 2008.