STU
FEI

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY
A INFORMATIKY

2011

# INSTITUTE OF COMPUTER SCIENCE AND MATHEMATICS

Annual Report
Slovak University of Technology in Bratislava

# INSTITUTE OF COMPUTER SCIENCE AND MATHEMATICS

**http://www.fei.stuba.sk/**

**Director of the Institute:**
**prof. RNDr. Otokar Grošek, PhD.**

Tel.: +421-2-602 91 226 / Fax: +421-2-654 20 415
E-mail: otokar.grosek@stuba.sk

**Deputy director:** doc. RNDr. Ľubomír Marko, PhD.
Tel: +421-2-654 27 351, e-mail: lubomir.marko@stuba.sk
Fax: +421-2-654 20 415
**Institute Secretary:** RNDr. Elena Pastuchová, PhD.
Tel.: + 421-2-602 91 303, E-mail: elena.pastuchova@stuba.sk
Fax.: + 421-2-654 20 415
**Head of Administration Office:** Zuzana Šabíková
Tel: +421-2-602 91 266, E-mail: zuzana.sabikova@stuba.sk
Fax: +421-2-654 20 415

## General Information

On May 1, 2011 was established the Institute of Computer Science and Mathematics as a union of two former Departments at FEI STU, namely Department of Informatics and Information Technology and Department of Mathematics. In fact we can count our history from the creation of the Department of Applied Informatics and Information Technology at FEI STU on Feb 1, 2004. During this short period have finished 459 Bachelors, 191 Masters (Engineers) and 6 PhD students. The study program Applied Informatics possesses deep theoretical and methodological knowledge and practical skills from the essential areas of the core of Informatics. Further knowledge from measurement, data capture, processing and transmission of information, and diagnostic of systems is included in the program. A graduate will also have knowledge about information and communication networks, will understand methods of modelling and simulation of systems and processes. To achieve this target, courses from the core fields of Information Systems and Software Engineering interlace with courses divided into four majors: Security of Information Technologies, Biometrics, Modelling and Simulation of Event Systems, and IT in Control and Decision Making. During the study principles of individual and team scientific work and research, formulation of problems, their solution and presentation are emphasized, respectively. A broad professional career in the different branches of science, research, industry and services is open for graduates, like auditing large information and communication systems, design security systems to protect sensitive data, modelling of work-flow processes, and embedded systems, and design and use information systems and software products in the area of control engineering in various practical application domains. The Institute consists of 3 Departments, namely Department of IT Security, Department of Software Engineering and Department of Mathematics.

## Departments of Institute of Computer Science and Mathematics

### Department of IT Security

**Department chair:** doc. Ing. Pavol Zajac, PhD.
Tel: +421-2-602 91 181, E-mail: pavol.zajac@stuba.sk
Fax: +421-2-654 20 415

**Short history**

The cryptology education at EF SVŠT began in 1984 with a course "Secret communication in computer networks" for postgraduate study (PhD) as the first in former Czechoslovakia. In 1986 O. Grošek (EF SVŠT) and K. Nemoga (MÚ SAV) established a new research seminar CRYPTO, and except a short break 1989-1993, it has still been a main center of cryptology research at FEI STU. In 1995 started a course Ciphering for students, along with the first Bachelor's projects and Diploma Theses in this area. Since the same year we have had graduate students in the field of 25-11-9 Applied Informatics, and also (since 1997) 11-14-9 Applied Mathematics with the major Crytology.

Since 2000/01 at the Department of Mathematics, and in cooperation with the former Department of Applied Informatics and Information Technology, we have had the first Masters degree students in the field of Security of Information Technologies. After the creation of FIIT STU in 2003, the cryptology group of prof. Grošek created a core of the Department of Applied Informatics and Information Technology at FEI STU on Feb 1, 2004. On May 1, 2011 was established the Institute of Computer Science and Mathematics as a union of two former Departments at FEI STU. Since that time Crypto-group has formed the core of the Department of IT Security.

**Awards 2011**

KEYMAKER student competition (Santa's Crypto, Prague, Dec. 1-2, 2011):
Radoslav Čagala: Algebraic cryptanalysis of GOST, winner of Diploma Thesis category
Viliam Hromada: Fault Analysis of Stream Ciphers (with M. Vojvoda), the absolute winner

**Activities 2011**

Oct 3 - 6, 2011: Workshop: Graph Theory and Interconnection Networks
International project: Cryptographic algorithms and primitives with increased resistance of side-channel attack (CAPRI), with Laboratoire Hubert Curien, UMR 5516 CNRS, Université Jean Monnet Saint-Etienne, France
Weekly during semester:
Seminar CRYPTO, Invited lectures: prof. P. Horak, University of Washington,Tacoma, USA, L. Gaspar, Lab. Hubert Curien, France
Directions, Future Trends, and Priorities
Organization of Central European Conference on Cryptology 2012.

1. Increased grant funding of the department.
2. Continual improvement of educational processes.
3. Involvement of MSc. students in the cryptology research.
4. Cooperation with governmental agencies and enterprise in education and research.

## Department of Software Engineering

**Department chair:** doc. RNDr. Gabriel Juhás, PhD.
Tel: +421 -2-602 91 135, E-mail: gabriel.juhas @stuba.sk
Fax: +421-2-602 91 415

**Short history**

History of the Department of Software Engineering began in February 2004 along with the development of the Department of Applied Informatics and Information Technology to teach students in the field of Advanced Web Technology. In September 2005 there was established a group of associated professor Juhás working in modelling, analysis, synthesis and verification of a wide range of event systems in various application areas. Other fields of research are architecture and software development, biometrics, eHealth and telemedicine. In 2009 the first Masters degree student in the field of Modelling and Synthesis of Event Systems finished. In 2011 the group became a part of the Institute of Computer Science and Mathematics, and was named Department of Software Engineering.

**Activities 2011**

December 2011 – Opening of the National Centre of Telemedicine Services with IBM, WHO, and Slovak Medical Chamber as the partners.

**Directions, Future Trends, and Priorities**

Telemedicine represents innovative shift in delivering medical services with application of information and communication technologies outside the health institutions. Applications of telemedicine services include mobile and wearable technologies to support tele-health for management of chronic conditions and support general well being from infants to elderly. Other domains of telehealth systems research (including nonclinical domains) are in the scope of ongoing efforts to create the ground for identification and discussion of technological, social, cultural, economic and other drivers to gain wide acceptability of telemedicine services and systems.

National Centre of Telemedicine Services (NCTS) was opened on 1. 12. 2011 at Slovak University of Technology in Bratislava, Faculty of Electrical Engineering and Information Technology (FEI STU). Strategic partner of the NCTS is IBM Slovakia with important support to the Centre from Slovak Medical Chamber and WHO office in Slovakia.

Research and development in the Centre is aimed at the "complete loop system" including remote data collection (biomedical telemetry devices), data transmission and analytics to support experts review and feedback to medical personnel and the patients. International state-of-the-art in related research domains is delivered through the close collaboration with distinguished experts in the field of biomedical engineering and health informatics – prof. Cerutti, prof. Allen, prof. Zhang (CUHK, China), prof. Akay (UH, USA) and other researchers grouped under NCTS's Scientific Advisory Board.

Tele-monitoring services are developed by the NCTS with close cooperation with its medical partners include acquisition of vital signs related to, e.g. blood pressure, body temperature, glycemia, ECG. The complex picture of patient status is completed with GPS data and VOIP teleconsultations. Management of patient conditions is supported by clinicians' applications related to management of acquired data and alarm generation supporting the prompt feedback to the patient and provision of professional help. The specific characterization of application is based on the requirements of medical personnel, related clinical process and target group (for example diabetes management, elderly citizens).

## Department of Mathematics

**Department chair:** doc. RNDr. Ľubomír Marko, PhD.
Tel: +421-2-654 27 351, E-mail: lubomir.marko@stuba.sk
Fax: +421-2-654 20 415

The Origin of the Department of Mathematics is the same as the origin of the Slovak Technical School of M. R. Štefánik (1938) and the first rector was mathematician Jur Hronec too. In 1951 the Institutes of mathematics were united into the unique Department of mathematics of Slovak University of Technology (SVŠT), which was associated to Faculty of Electrical Engineering of SVŠT (EF SVŠT). The first head of the Department of Mathematics became academician Š. Schwarz. In 1984 the residence of EF SVŠT moved to Mlynská dolina (Bratislava). We remember famous researchers being employed at the Department, namely professors Hronec, Schwarz, Jakubík, Švec, Greguš, Mišík, Kluvánek, Riečan, Znám, Eliáš, Ivan, Šulka, Gatial, Porubský, Horák, Riečanová. In 2011 the Department of mathematics was incorporated to the Institute of Informatics and Mathematics.

History of the Department of Software Engineering began in February 2004 along with the development of the Department of Applied Informatics and Information Technology to teach students in the field of Advanced Web Technology. In September 2005 there was established a group of associated professor Juhás working in modelling, analysis, synthesis and verification of a wide range of event systems in various application areas. Other fields of research are architecture and software development, biometrics, eHealt and telemedicine. In 2009 has finished the first Masters degree students in the field of Modelling and Synthesis of Event Systems. In 2011 the group became a part of the Institute of Computer Science and Mathematics, and was named Department of Software Engineering.

# I. STAFF

**Professors:**
prof. RNDr. Otokar Grošek, PhD., prof. RNDr. Igor Bock, PhD.
prof. RNDr. Zdenka Riečanová, PhD.

**Associate Professors**
doc. RNDr. Jaroslav Fogel, PhD., doc. RNDr. Gabriel Juhás, PhD.,
doc. RNDr. Karol Nemoga, PhD., doc. Dr. Ing. Miloš Oravec,
doc. Ing. Pavol Zajac, PhD. , doc. RNDr. Ľubomír Marko, PhD.,
doc. RNDr. Vladimír Olejček, PhD., doc. RNDr. Boris Rudolf, PhD.,
doc. RNDr. Ladislav Satko, PhD., doc. RNDr. Peter Volauf, PhD.,
doc. RNDr. Michal Zajac, PhD.

**Assistant Professors:**
Ing. Štefan Balogh, Ing. Alexander Hambalík, PhD., Ing. Matúš Jókay, PhD.,
RNDr. Igor Kossaczky, CSc., RNDr. Eva Kostrecová, PhD., Ing. Fedor Lehocki, PhD.,
Mgr. Marek Sýs, PhD., Mgr. Zuzana Ševčíková, Ing. Milan Vojvoda, PhD.,
RNDr. Igor Brilla, PhD., RNDr. Karla Čipková, PhD.,RNDr. Mária Kečkemétyová, PhD.,
RNDr. Hana Lichardová, PhD., RNDr. Ivica Marinová, PhD.,
Mgr. Dávid Pancza, PhD.,RNDr. Elena Pastuchová, PhD.,
Mgr. Marcel Polakovič, PhD., Mgr. Michal Zákopčan, PhD.

**Research Workers:**
Ing. Ondrej Gallo, Ing. Stanislav Marček

**Technical Staff:**
Zuzana Šabíková (Head)
Brigita Timková, Gabriela Grúňová (secretary)

**PhD. Students:**
Ing. Eugen Antal, Ing. Michal Braško, Ing. Lucia Cibulková,
Ing. Matej Féder, Ing. Jaroslav Hamráček, Ing. Viliam Hromada,
Ing. Igor Kazlov, Ing. Ján Mazanec, Mgr. Michal Mikuš, Ing. Ľuboš Omelina,
Ing. Filip Pilka, Ing. Marek Repka, Ing. Martin Riesz, Ing. Andrej Savka,
Ing.Juraj Varga, Ing. Milan Zelina, Mgr. Viktória Rozborová,
Mgr. Tomáš Žilka, Mgr. Andrea Tinajová

# II. EQUIPMENT

## II. 1 Teaching and Research Laboratories

- IT Sec Laboratory
- DIEDC - Database Information Education and Demonstration Center
- Laboratory of Medical Informatics
- Laboratory of Communication Networks
- Experimental Laboratory of Institute

## II. 2 Special Measuring Instruments and Computers

- HP Proliant ML 150
  2x CPU INTEL XEON 2,8 GHz
  RAM 12 GB
  HDD 35 GB
- MSDN Academic Alliance (MSDN AA) = Microsoft Developers Network Academic Alliance

# III. TEACHING

## III.1 Undergraduate Study (Bc.)

Subject, semester, hours per week for lectures and for seminars or practical exercises, name of the lecturer:

| | |
|---|---|
| Algorithms and Programming<br>(1st sem., 3-2 h) | P. Zajac |
| Algorithms and Programming<br>(1st sem., 3-2 h) | M. Sýs |
| Algorithms and Programming<br>(1st sem., 3-2 h) | I. Kossaczký |

Analysis and Complexity of Algorithms
5th sem., 3-1 h) M. Vojvoda

Classical Ciphers
(4th sem., 2-2 h) O. Grošek

Database Systems
(3rd sem., 3-2 h) M. Vojvoda

Operating Systems
(3rd sem., 3-2 h) M. Jókay

Programming Techniques
(2nd sem., 3-2 h) I. Kossaczký

Designing of Database Systems
(4th sem., 3-1 h) G. Juhás

Information Security
(5th sem., 2-2 h) E. Kostrecová

Computer Crimes
(6th sem., 2-2 h) E. Kostrecová

Modelling in Software Engineering
(5th sem., 2-2 h) J. Hanák

Introduction to Cryptography
(5th sem., 2-2 h) O. Grošek

Fast Algorithms
(6th sem., 2-2 h) K. Nemoga

Introduction to Computer Science
(4th sem., 3-2 h) O. Grošek

Communication Networks 1
(4th sem., 3-1 h) M. Oravec

Software Application Development 1
(3rd sem., 2-2 h ) M. Šrámka

Software Architecture
(5th sem., 2-2 h ) G. Juhás

Management of IT Projects
(6th sem., 2-2 h) F. Lehocki

Workflow Management Systems
(6th sem., 2-2 h) F. Lehocki

Communication Networks 2
(6th sem.,4-1 h) A.Hambalík/M. Oravec

Calculus I
(1st sem., 4-2h) M. Kečkemétyová,
B. Rudolf, L. Satko

Logic Systems
(1st sem., 4-1h) V. Čerňanová, V. Olejček,
M. Polakovič

Calculus II
(2nd sem., 4-2h) I. Brilla, B. Rudolf, L. Satko

Linear Algebra I
(1st sem., 2-2h) M. Zajac

Calculus III
(3rd sem., 3-2h) Ľ. Marko

Ordinary Differential Equations
(3rd sem., 2-2h) Ľ. Marko

Discrete Mathematics and Logic
(3rd sem., 3-2h) I. Marinová

Numerical and Statistical Computation
(3rd sem., 3-2h) P. Volauf

Numerical and Statistical Computations
(4th sem., 3-2h) V. Olejček

Statistical Methods in Informatics
(4th sem., 2-2h) E. Pastuchová

Probability and Statistics
(4th sem., 2-2h) P. Volauf

Linear Algebra and Linear Programming
(6th sem., 2-2h) M. Zajac

## III.2 Graduate Study (Ing.)

Computer Graphics
(1st sem., 3-2 h) M. Sýs

Object-Oriented Programming
(3rd sem., 3-2 h) V. Novák

Ciphers in Communication Networks
(1st sem., 3-2 h) K. Nemoga

Modelling and Simulations of Event Systems
(1st sem., 3-2 h) G. Juhás

Practice of Security of Information Systems
(1st +3rd sem., 3-2 h) M. Zanechal

Formal Methods
(1st sem., 3-2 h) J. Fogel

Cryptanalysis
(3rd sem., 3-2 h) M. Vojvoda, M. Sýs, P. Zajac

Analysis and Synthesis of Event Systems
(2nd sem., 3-2 h) G. Juhás

Biometrics
(2nd sem., 3-2 h) M. Oravec

System Programming
(2nd, 4th sem., 3-2h) J. Fogel

Design of Ciphers
(3rd sem., 3-2 h) P. Zajac

Machine Learning and Neural Networks
(1st sem., 3-2h) M. Oravec

Workflow Management Systems, Processes and Web Services
(2nd sem., 3-2 h) F. Lehocki

Coding Theory
(1st sem., 3-1h) K. Čipková

Partial Differential Equations
(1st sem., 3-2h) I. Bock

Partial Differential Equations Numerical Methods
(1st sem., 2-2h) I . Bock

Functional Analysis I
(1st sem., 2-2h) M. Zajac

Differential and Difference Systems
(1st sem., 2-2h) B. Rudolf

Numerical Solutions of Differential Equations
(1st sem., 2-0h) I. Bock

Stochastic Models
(2nd sem., 2-2h) V. Olejček

Mathematics
(1st sem., 3-2h) I. Bock

Difference and Differential Equations
(1st sem., 2-2h) B. Rudolf

Theory of Fuzzy Systems
(1st sem., 3-2h) P. Volauf

### III.3 Undergraduate and Graduate Study for Foreign Students (in English Language)

| | |
|---|---|
| Algorithms and Programming (1st sem., 12 h consul.) | J. Varga |
| Programming Techniques (2nd sem., 12 h consul.) | M. Sýs |
| Databases Systems (1st sem., 12 h consul.) | Ľ. Omelina |
| Computer Architecture (2nd sem., 12 h consul.) | M. Jókay |
| Business Management (2nd sem., 12 h consul.) | F. Lehocki |
| Classical Ciphers (4th sem., 12 h consul.) | O. Grošek |

### III.4 Distance Study

| | |
|---|---|
| Algorithms and Programming (1st sem., 6x2 h consul.) | A. Hambalík |

### III.5 Undergraduate Study (Bc. Distance Education Method)

| | |
|---|---|
| Mathematics I (1st year) | Ľ. Marko |
| Logic Systems (1st year) | D. Pancza |
| Mathematics II (1st year) | I. Brilla |
| Mathematics III (2nd year) | Ľ. Marko, P. Volauf |
| Mathematics IV (2nd year) | V. Olejček |

### III.6 Graduate Study (Ing. Distance Education Method )

| | |
|---|---|
| Mathematics (1st year) | I. Bock |

### III.7 Postgraduate Study

| | |
|---|---|
| Numerical Solutions of Differential Equations (1st sem., 2-0 h) | I. Bock |

## IV. RESEARCH PROJECTS

### IV.1 National Scientific Projects

- Solution of Current Problems in Cryptology, VEGA 1/0244/09. Duration: 1. 1. 2009 – 31. 12. 2011(completed) (O. Grošek)
- Modernization of Education Process in Basic and Grammar Schools., ITMS: 26110130083, 26140130013 and ITMS: 26110130084, 26140130084, certified lector in the project, Duration: 2008–2013 (solved) (A. Hambalík)
- Proposal of Methods of Analysis and Classification for Biometric Recognition of Human Faces and Traffic in Communication Networks, VEGA 1/0214/10. Duration: 01. 01. 2010 - 31. 12. 2011 (completed) (M. Oravec)
- Centre of Excellence of SMART Technologies, Systems and Services ITMS: 26240120005 Duration: 01. 05. 2009 – 30. 04. 2011 (completed) (G. Juhás)
- Centre of Excellence of SMART Technologies, Systems and Services II ITMS: 26240120029 Duration: 01. 01. 2010 – 31. 12. 2012 (solved). (G. Juhás)
- Measuring, communication and information systems for monitoring of cardiovascular risk in hypertension patients APVV 0513-10 Duration: 1. 05. 2011- 30. 06. 2014 (started) (F. Lehocki)
- The analysis of quasistatic dynamic contact problems of mechanics.VEGA 1/0021/10. Duration: 01. 01.2010 – 31. 12. 2011(completed) (I. Bock)
- Modelling uncertainty quantum structures, states, fuzzy relations and evaluators with application in the Probability Theory. VEGA 1/0297/11. Duration: 01. 01. 2011 – 31. 12. 2014 (started) (Z. Riečanová)

### IV.2 International Scientific Projects

- ERASMUS Educational Project, Bilateral Agreement, University of La Laguna, Spain Duration: 09. 10. 2006 – 30. 06. 2012 (solved) (O.Grošek)
- Cryptographic Algorithms and Primitives with Increased Resistance Against Side
- Channel Attacks, Project SK-FR-0011-09. Duration: 25. 02. 2010 – 20. 12. 2011(completed) (O. Grošek)

## V. COOPERATION

### V.1 Cooperation in Slovakia

- National Security Authority, Bratislava
- Faculty of Mathematics, Physics and Informatics, Comenius University, Bratislava
- Association of the Infovek Project, Ministry of Education of the Slovak Republic – Project of Informatization of Regional School – PIRŠ
- Slovak Research and Development Agency, Bratislava
- Faculty of Chemical and Food Technology, STU, Bratislava
- Technical University, Zvolen
- J. Selye University, Komárno
- Bratislava Metodical and Pedagogical Centre
- Trenčín Metodical and Pedagogical Centre
- Virtual Academy of Bratislava Self-Governing Region
- University of Constantin the Philosopher, Nitra
- Department of Engineering Pedagogy and Psychology, MtF STU Bratislava
- Ministry of Finance of the SR
- Institute of Measuremet, Slovak Academy of Sciences, Bratislava
- Slovak Standards Institute
- Ministry of Health of the SR, Strategic Targets of Health
- Security Authority of the Ministry of Defence of the SR

- Institute of Forensic Science of Police Corps, Bratislava
- ÚIPŠ Bratislava
- Elfa, Ltd. Košice
- Datalan, Ltd. Bratislava
- Centre of Distance Education (SDV ICV CUP REK), Bratislava
- Centire, Ltd. Bratislava
- Mathematical Institute, Slovak Academy of Sciences, Bratislava
- Faculty of Management, Comenius University, Bratislava
- Department of Mathematics and Descriptive Geometry, Faculty of Civil Engineering, STU, Bratislava
- Department of Structural Mechanics, Faculty of Civil Engineering, STU, Bratislava
- Department of Mathematical Analysis, FMPI, Comenius University, Bratislava
- Department of Mathematics, Armed Forces Academy, Liptovský Mikuláš
- Department of Mathematics, Faculty of Mechanical Engineering, STU, Bratislava
- Institute of Information Engineering, Automation and Mathematics, Faculty of Chemical and Food Technology, STU, Bratislava

## V.2 International Cooperation

- Institute of Informatics, Academy of Sciences of the Czech Republic, Prague, CR
- University of LA LAGUNA, Department of Statistics, Operations Research and Computing, Tenerife, Spain
- Department of Information Systems Security, Concordia University College of Alberta, Canada
- Faculty of Informatics MU Brno, CR
- Department of Mathematics, Faculty of Electrical Engineering, ČVUT Prague, CR
- Lehrstuhl für Angewandte Informatik, Katholische Universitaet Eichstätt-Ingolstadt, Germany
- Fachgruppe Simulation und Modellierung, Institut für Systems Engineering, Universitätt Hannover, Germany
- Florida Atlantic University, Boca Raton, Florida, USA
- Department of Mathematics, University of Washington, Tacoma, Washington, USA
- Institute for Experimental Mathematics, University of Essen, Germany
- Department of Mathematics and Science, Indiana State University, USA
- Eszterházy Károly College, Eger, Hungary
- AINTEK A.E, Greece
- Virginia Tech, Blacksburg, Virginia, USA
- McMaster University, Hamilton, Canada
- University of Waterloo, Canada
- University of Toronto, Canada
- Universität Ausgsburg, Germany
- Institut for Informatikk, Universitetet i Bergen, Norway
- Laboratoire Hubert Curien, Université Jean Monnet, Saint –Etienne, France
- Ecole Nationale de Police, Montbéliard, France
- Technische Universiteit Eindhoven, Eindhoven, The Netherlands
- University of Southampton, UK
- MINT, Emmy Noether Verein, Ulm, Germany
- Institut für Algebra und Computermathematik TU Vienna, Austria
- Department of Mathematics, FEE CTU, Prague, CR
- Academy of Sciences of the Czech Republic, Prague, CR
- Department of Mathematics, Faculty of Natural Sciences of MU, Brno, CR
- Institut de Mathématique, Université Louis Pasteur, Strasbourg, France
- Math. Institute, Polish Academy of Sciences, Warsaw, Poland
- University of Ljubljana, Slovenia
- Institute of Nuclear Physics, Academy of Sciences of the Czech Republic ,
- Rez near Prague, CR
- Department of Mathematics, Zhejiang University Hangzhou, China

## V.3 Contracts

none

# VI. THESES

## VI.1 Masters Theses

Masters theses supervised at the Institute of Computer Science and Mathemetics. The names of supervisors are in brackets.

[1] E. Antal: Selected Problems in Cryptanalysis of Fialka M-125 cipher (O. Grošek)

2] T. Zaťko: Qualified electronic signature in the Slovak Republic and European Union (O. Grošek)

[3] M. Dubovský: Protection of laser show (M.Sýs)

[4] B. Šulej: Methods for direct computer memory Access (Š. Balogh)

[5] T. Marko: Palmprint feature extraction (L. Adamko)

[6] T. Straka: Cryptography strong random numbers generators (L. Adamko)

[7] M. Bella: The attack against hash function MD4 (M. Vojvoda)

[8] J. Hribik: Verifiable Secret Sharing Schemes (K. Nemoga)

[9] J. Varga: Linear Recurring Sequences over Zm (K. Nemoga)

[10] J. Štefanička: Tools misused at cracking (E. Kostrecová)

[11 L. Pír: Inteligent Camera Systems in Objects Security (M. Kempný)

[12] M. Paulínyi: Protection against spamming (E. Kostrecová)

[13] V. Hromada: Fault Analysis of Stream Ciphers (M.Vojvoda)
14] R. Blaško: Use of artificial intelligence in medical diagnosis of the patient (M. Oravec)
[15] J. Režnák: Face recognition in biometrics using kernel methods KPCS and GDA (M. Oravec)
[16] J. Baroš: Degree of video damage after insertion to public repository for anonymous sharing of multimedia content (M. Jókay)
[17] R. Čagala.: Algebraic cryptanalysis of the GOST cipher (P. Zajac)
[18] M. Plančík: Algebraic cryptanalasis of Serpent (P. Zajac)
[19] M. Páleníková: Cube attack (P. Zajac)
[20] M. Hrušovský: Security Prevention for Customers against Internet Banking Crime (Z. Ševčíková)
[21] M. Kováč: Deadlock states analysis in Petri Net (Z. Ševčíková)
[22] M. Mádel: Transformation of workflow processes into Petri nets (Z. Ševčíková)
[23] R. Jadrončík: Identification of programs from nonsequential behavior (G. Juhás)
[24] S. Lucký: Dynamical soundness analysis of Petri nets (G. Juhás)
[25] S. Madaras: Opportunities for transformation Workflow models into Petri Nets (G. Juhás)
[26] L. Oles: Petri net synthesis (G. Juhás)
[27] M. Rástocký: Analysis of Processes with Dynamic Resource Allocation (G. Juhás)
[28] M. Marko: Web portal for e-learning CMS Joomla (M. Foltin)
[29] M. Súlovec: Creation of framework for network client-server communication model (Ľ. Stuchlíková)
[30] T. Búgel: Automated recognition system for authenticity of digital images (A. Hambalík)
[31] M. Meszáros: Verification of concurrent programs written in C language (J. Fogel)
[32] J. Plevko: Constructing Büchi Automatas from LTL formulas (J. Fogel)
[33] M. Veselý: Universal software tester of active components of local area networks (A. Hambalík)
[34] R. Lipovský: Virtualization against malware (Š. Balogh)
[35] M. Hochel: Proposal for a server – client application and the communication interface for an automatic warehouse management (J. Dorner)
[36] M. Gašparík: Capturing objects by camera and recognizing them (J. Dorner)
[37] F. Drugda: Information system for electronic prescription drug from doctor view (Š. Balogh)
[38] M. Dzúrik: Implementation of National Health Portal (Š. Balogh)
[39] B. Botto: System for creating the interactive courses which fulfills the needs of Slovak health (F. Lehocki)
[40] E. Buček: Creation of library package for development of 3D grafics applications (Ľ. Stuchlíková)
[41] A. Cvečko: Architecture of EHR (F. Lehocki)
[42] M. Kováč: Telemedicine applications in healthcare (F. Lehocki)
[43] L. Kuba: Models of diagnostic systems (F. Lehocki)
[44] D. Tekeljak: Remote administrator access to the managed server secured by biometrics (A. Hambalík)
[45] M. Hatala: Utilizing modern ICT in rehabilitation of patients (F. Lehocki)
[46] M. Hurňák: Transformation from VHDL Model into Petri Nets (O. Gallo)
[47] M. Kaša: Transformation of time behavior of logic circuit in Petri nets (O. Gallo)
[48] L. Cibulková: Modelling of Workflow Processes (O. Gallo)
[49] Ľ. Belicová: Modelling and analysis of Workflow Processes (O. Gallo)
[50] J. Vlk: Academic information system based on platform J2EE ( V. Novák)
[51] T. Gallovič: Logistics system for android platform (V. Novák)

### VI.2 PhD. Theses

[1] M. Jókay: Steganography in the Images and Video (O. Grošek)
[2] F. Lehocki: Models of Diagnostic Systems (G. Juhás)

### VI.3 Habilitation Theses

[1] P. Zajac: Contribution to the design and cryptanalysis of ciphers, STU 2011.

## VII. OTHER ACTIVITIES

- Seminar Crypto (O. Grošek)
- Reviewer of ZentralblattMath (K. Nemoga, O. Grošek)
- Seminar: Machine Learning (M.Oravec)
- Seminar: Topologies and states on quantum structures (Z. Riečanová)
- Seminar: Variational inqualities and optimal control on mechanics (I. Bock)
- Seminar: Ordinary differential equations (B. Rudolf )
- Seminar: Numerical methods of solutions of differential equations - seminar for postgraduate students (I. Bock)
- Organising of 8th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal control in Nemecká, 5 -10 september 2011 (I. Bock , B. Rudolf, M. Zajac)

# VIII. MEMBERSHIP IN INSTITUTIONS/ COMMITTEES

## VIII.1 Membership in National Institution/Committees

- Member of – SSKI – Slovak Society for Cybernetics and Informatics
- JSMF- Union of Slovak Mathematicians and Physicists (J. Fogel)
- Member of – JSMF (O. Grošek)
- Member of – JSMF (K. Nemoga)
- Member of – SBIMI - Society of Biomedical Engineering and Medical Informatics (F. Lehocki)
- Member of – TC 37 of SÚTN (Slovak Standards Institute) (F. Lehocki)
- Member of – JSMF (I. Bock, M. Kečkemétyová, I. Marinová, V. Olejček, P.Volauf
- E. Pastuchová, B. Rudolf, M. Polakovič, Z. Riečanová, L. Satko, M. Zajac)
- Member of – Slovak Society for mechanics (I. Bock, I. Brilla, Ľ. Marko)
- Member of – Slovak Statistical and Demographic Society (E. Pastuchová)
- Member of- Mathematica Slovaca, Springer (editors: I. Bock, M. Zajac)

## VIII.1 Membership in International Institution/Committees

- Member of AMS – American Mathematical Society (O. Grošek, I. Bock, V. Olejček, Z. Riečanová)
- Member of SIAM – Society for Industrial and Applied Mathematics (O. Grošek, V. Olejček, L. Satko)
- Member of IEEE - (Institute of Electrical and Electronics Engineers) Computer Society (J. Fogel)
- Member of IACR - International Association for Cryptologic Research (K. Nemoga)
- Member of - IEEE (Institute of Electrical and Electronics Engineers) Institution of Engineering and Technology (M. Oravec)
- Member of - The European Association for the Transfer of Technologies, Innovation and Industrial Information (F. Lehocki)
- Member of (Institute of Electrical and Electronics Engineers) Engineering in Medicine and Biology Society (F. Lehocki)
- Member of – ETIS European Transport policy Information System (E. Kostrecová)
- Member of ISIMM - International Society for the Interaction of Mechanics and Mathematics (I. Brilla)
- Member of IQSA - International Quantum Structures Association (Z. Riečanová, V. Olejček, G. Jenča)
- Member of Bernoulli Society (Z. Riečanová, V. Olejček)
- Member of IACM - International Association for Computational Mechanics (I. Brilla, Ľ. Marko)
- Member of - Emmy Noether Society (Z. Riečanová, I. Marínová, E. Pastuchová, G. Jenča)
- Member of - GAMM - Gesellschaft für Angewandte Mathematik und Mechanik (I. Bock)
- Member of - ISSMO - Society for Structural and Multidisciplinary Optimization (I. Bock)
- Membership in Editorial Boards of International Journals
- Member of - Tatra Mountains Mathematical Publications, publisher: Mathematical Institut of SAS, (O. Grošek)
- Member of - Tatra Mountains Mathematical Publications, publisher: Mathematical Institut of SAS, (K. Nemoga – managing editor)
- Member of - Zentralblath Math, publisher: De Gruyter, (K. Nemoga - managing editor of the Slovak Unit)
- Member of - Journal of Mathematical Cryptology, (O. Grošek)
- Member of - Central European Journal of Computer Science (CEJCS), publisher: Versita, co-published with (Springer Verlag, (M. Oravec – editor)
- Member of - Transactions on Petri Nets and Other Models of Concurrency (Publisher: Springer Verlag (G. Juhás)
- Member of -Tatra Mountains Mathematical Publications, SAS (editor: Z. Riečanová)

Our students are trying to break ECC cryptosystem by side-channel attack.

International conference - 8th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control in Nemecká, Slovakia, Sept. 5–10, 2011.

Ing. Viliam Hromada, the absolute winner of KEYMAKER student competition at Santa's Crypto, Prague, Dec. 1-2, 2011 is getting diploma as "Absolute winner" of all the categories.

# IX. PUBLICATIONS

## IX. 1 Journals

[1] ANTAL, E. - JÓKAY, M.: Rotor Cipher Machine Fialka M-125: Implementation and Utilization. In: Crypto-World. - ISSN 1801-2140. - Vol. 13, No. 9 (2011), p. 9-15. (in Slovak)

[2] ANTAL, E. - JÓKAY, M.: Rotor Cipher Machine Fialka M-125: The Selected Characteristics of the Cipher. In: Crypto-World. - ISSN 1801-2140. - Vol. 13, No. 6 (2011), p. 23-32. (in Slovak)

[3] ANTAL, E. - JÓKAY, M.: Rotor Cipher Machine Fialka M-125. Machine Design. In: Crypto-World. - ISSN 1801-2140. - Vol. 13, No. 4 (2011), p. 18-27. (in Slovak)

[4] ANTAL, E. - JÓKAY, M.: Rotor Cipher Machine Fialka M-125: The Comparison with Other Cipher Machines. In: Crypto-World. - ISSN 1801-2140. - Vol. 13, No. 5 (2011), p. 15-23. (in Slovak)

[5] ANTAL, E. - JÓKAY, M.: Rotor Cipher Machine Fialka M-125. Tutorial. In: Crypto-World. - ISSN 1801-2140. - Vol. 13, No. 4 (2011), p. 17. (in Slovak)

[6] BAN, J. - FÉDER, M. - ORAVEC, M. - PAVLOVIČOVÁ, J.: Non-Conventional Approaches to Feature Extraction for Face Recognition. In: Acta Polytechnica Hungarica. - ISSN 1785-8860. - Vol. 8, No. 4 (2011), p. 75-90. (in English)

[7] BENIAK, M. - PAVLOVIČOVÁ, J. - ORAVEC, M.: 3D Chrominance Histogram Based Face Localisation. In: International Journal of Signal and Imaging Systems Engineering. - ISSN 1748-0701 (on-line). - ISSN 1748-0698 (PRINT). - Vol. 4, Iss. 1 (2011), p. 3-12. (in English)

[8] BESSONOV, RV. - BRAČIČ, J. - ZAJAC, M.: Non-Hyperreflexive Reflexive Spaces of Operators. In: Studia Mathematica. - ISSN 0039-3223. - Vol. 202, Issue 1 (2011), p. 65-80. (in English)

[9] BOCK, I. - KEČKEMÉTYOVÁ, M.: An Optimal Design with Respect to a Variable Thickness of a Vuscoelastic Beam in a Dynamic Boundary Contact. In: Tatra Mountains Mathematical Publications. - ISSN 1210-3195. - Vol. 48 (2011), p. 15-24. (in English)

[10] BOCK, I. - JARUŠEK, J.: Unilateral Dynamic Contact Problem for Vicsoelastic Reissner-Mindlin Plates. In: Nonlinear analysis: Theory, Methods and Applications. - ISSN 0362-546X. - Vol. 74 (2011), p. 4192-4202. (in English)

[11] KALINA, M. - OLEJČEK, V. - PASEKA, J. - RIEČANOVÁ, Z.: Sharply Dominating MV-Effect Algebras. In: International Journal of Theoretical Physics. - ISSN 0020-7748. - Vol. 50 (2011), p. 1152-1159. (in English)

[12] KOSTRECOVÁ, E.: Initiatives of International Cooperation between States and International Institutions for the Protection of Electronic Space. In: Policajná teória a prax. - ISSN 1335-1370. - Vol. 19, No. 2 (2011), p. 134-138. (in Slovak)

[13] PASEKA, J. - RIEČANOVÁ, Z.: Considerable Sets of Linear Operators in Hilbert Spaces as Operator Generalized Effect Algebras. In: Foundations of Physics. - ISSN 0015-9018. - Vol. 41 (2011), p. 1634-1647. (in English)

[14] PASEKA, J. - RIEČANOVÁ, Z.: The Inheritance of BDE-Property in Sharply Dominating Lattice Effect Algebras and (o)-Continuous States. In: Soft Computing. - ISSN 1432-7643. - Vol. 15, No. 3 (2011), p. 543-555. (in English)

[15] PASTUCHOVÁ, E. - SABO, M. - KOHNOVÁ, S.: Comparison of Clustering Methods Applied to Hydrological Data. In: Forum Statisticum Slovacum. - ISSN 1336-7420. - Vol. 7, No. 7 (2011), p. 168-175. (in English)

[16] PILKA, F. - ORAVEC, M.: a NARX Neural Network Algorithm for Video Traffic Prediction. In: Journal of Electrical and Electronics Engineering (JEEE). - ISSN 1844-6035. - Vol. 4, No. 1 (2011), p. 179-184. (in English)

[17] PILKA, F. - ORAVEC, M.: Prediction Methods for MPEG-4 and H. 264 Video Transmission. In: Journal of Electrical Engineering. - ISSN 1335-3632. - Vol. 62, No. 2 (2011), p. 57-64. (in English)

[18] POLAKOVIČ, M.: Generalized Effect Algebras of Bounded Positive Operators Defined on Hilbert Spaces. In: Reports on Mathematical Physics. - ISSN 0034-4877. - Vol. 68, No. 2 (2011), p. 241-250. (in English)

[19] POLAKOVIČ, M. - RIEČANOVÁ, Z.: Generalized Effect Algebras of Positive Operators Densely Defined on Hilbert Spaces. In: International Journal of Theoretical Physics. - ISSN 0020-7748. - Vol. 50 (2011), p. 1167-1174. (in English)

[20] RACKO, J. - MIKOLÁŠEK, M. - BENKO, P. - HARMATHA, L. - GALLO, O. - GRANZNER, R. - SCHWIERZ, F.: Coupled Defect Level Recombination in th P-N Junction. In: Journal of Electrical Engineering. - ISSN 1335-3632. - Vol. 62, No. 6 (2011), p. 355-358. (in English)

[21] RIEČANOVÁ, Z. - ZAJAC, M. - PULMANNOVÁ, S.: Effect Algebras of Positive Linear Operators Densely Defined on Hilbert Spaces. In: Reports on Mathematical Physics. - ISSN 0034-4877. - Vol. 68, No. 3 (2011), p. 261-270. (in English)

[22] RIEČANOVÁ, Z.: Effect Algebras of Positive Self-Adjoint Operators Densely Defined on Hilbert Spaces. In: Acta Polytechnica. - ISSN 1210-2709. - Vol. 51, No. 4 (2011), p. 78-81. (in English)

[23] RIEČANOVÁ, Z. - ZAJAC, M.: Extensions of Effect Algebra Operations. In: Acta Polytechnica. - ISSN 1210-2709. - Vol. 51, No. 4 (2011), p. 73-77. (in English)

[24] RIEČANOVÁ, Z.: Lattice Effect Algebras Densely Embeddable into Complete Ones. In: Kybernetika. - ISSN 0023-5954. - Vol. 47, No. 1 (2011), p. 100-109. (in English)

[25] RIEČANOVÁ, Z. - PASEKA, J.: State Smearing Theorems and the Existence of States on Some Atomic Lattice Effect Algebras. In: Journal of Logic and Computation. - ISSN 0955-792X. - Vol. 21, No. 6 (2011), p. 863-882. (in English)

[26] RUDOLF, B.: on a Boundary Value Problem for Differential Equation with P-Laplacian. In: Tatra Mountains Mathematical Publications. - ISSN 1210-3195. - Vol. 48 (2011), p. 189-195. (in English)

[27] ZELINA, M. - ORAVEC, M.: Feature Selection for Application Recognition in Communication Networks. In: AD ALTA: Journal of Interdisciplinary Research. - ISSN 1804-7890. - Vol. 1, Iss. 1 (2011), p. 115-117. (in English)

### IX. 2 Conference Proceedings

[1] BALOGH, Š. - PONDELÍK, M.: Capturing Encryption Keys for Digital Analysis. In: IDAACS 2011: 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. Prague, Czech Republic, 15 - 17 September 2011. - Piscataway: IEEE, 2011. - ISBN 978-1-4577-1425-2. - p. 759-763. (in English)

[2] BALOGH, Š. - LEHOCKI, F. - JUHÁS, G.: EHealth in Slovakia and its Implementation. In: SMART S2AI: Workshop of SMART Systems and Services in Applied Informatics. Bratislava, Slovak Republic, 18 April 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3513-1. - p. 11-13. (in Slovak)

[3] BALOGH, Š. - CHOVANČÁK, D.: Using Data Mining Techniques for Detection Malware and Network Attacks. In: Knowledge 2011: 10th Conference. Stará Lesná, Slovak Republic, 31. 1. - 2. 2. 2011. - Ostrava: Technical University of Ostrava, 2011. - ISBN 978-80-248-2369-0. - p. 255-258. (in Slovak)

[4] BAN, J. - FÉDER, M. - ORAVEC, M. - PAVLOVIČOVÁ, J.: Enhancement of One Sample per Person Face Recognition Accuracy by Training Sets Extension. In: Proceedings ELMAR-2011: 53rd International Symposium. 14-16 September 2011, Zadar, Croatia. - Zadar: Croatian Society Electronics in Marine, 2011. - ISBN 978-953-7044-12-1. - p. 25-28. (in English)

[5] BLAŠKO, R. - ORAVEC, M. - PAVLOVIČOVÁ, J. - HANÚSKOVÁ, V. - LEHOCKI, F.: Image Preprocessing for Diagnostics Support in Ophtalmology. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 17, Special Issue: ELOSYS, Trenčín, 11.-14. 10. 2011, p. 5-8. (in English)

[6] BOCK, I.: Dynamic Contact Problems for Shells with Moderately Large Deflections. In: IUTAM Symposium on Dynamics Modelling and Interaction Control in Virtual and Real Environments. - Dordrecht: Springer, 2011. - ISBN 978-94-007-1642-1. - p. 293-300. (in English)

[7] BOCK, I. - JARUŠEK, J.: on a Dynamic Contact Problem for a Geometrically Nonlinear Viscoelastic Shell. In: 8th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control: Nemecká, Slovak Republic, September 5-10, 2011. - Bratislava: STU, 2011. - p. 3-7. (in English)

[8] BOCK, I. - LOVÍŠEK, J.: on Optimal Design of Plates in a Dynamic Contact with a Winkler Foundation. In: New Trends in Statics and Dynamics of Buildings: 9th International Conference. Bratislava, Slovak Republic, 20.-21. 10. 2011. - Bratislava: STU, 2011. - ISBN 978-80-227-3572-8. - p. 15-16. (in English)

[9] BRAŠKO, M.: on Comparison of Stream Ciphers Proposals in eStream Project. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 17, Special Issue: ELOSYS, Trenčín, 11.-14. 10. 2011, p. 189-193. (in English)

[10] BRILLA, I.: Numerical Analysis of Boundary Inverse Problems for Two Dimensional (2D) Orthotropic Solids. In: XXXII CILAMCE: Congresso Ibero Latino Americano de Métodos Computacionals em Engenharia. Ouro Preto, Brazil, 13-16 November 2011. - Sao Paulo, 2011. - CD-Rom. (in English)

[11] CIBULKOVÁ, L. - LEHOCKI, F.: Modelling of Workflow Processes. In: ŠVOČ 2011: Proceedings of Selected Works. Bratislava, Slovak Republic, 4. 5. 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3508-7. - p. 30-33. (in Slovak)

[12] CIBULKOVÁ, L. - LEHOCKI, F. - HANÚSKOVÁ, V. - ORAVEC, M. - PAVLOVIČOVÁ, J.: Clinical Workflow Modelling in Healthcare. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 17, Special Issue: ELOSYS, Trenčín, 11.-14. 10. 2011, p. 194-198. (in Slovak)

[13] ČERŇANOVÁ, V.: Card Game "Happy Families". In: Two Days with Didactics of Mathematics 2011: Prague, Czech Republic, 17. -18. 2. 2011. - Prague: JČMF, 2011. - ISBN 978-80-86843-32-2. - p. 29-32. (in Slovak)

[14] ČERŇANOVÁ, V.: The Use of the Scalar Product of the Vectors on the Shaping and Strenghtening of the Argumentative Skills of Pupils. In: Acta Mathematica 14. Nitra, Slovak Republic, 22.-23. September 2011. - Nitra: Constantine the Philosopher University in Nitra, 2011. - ISBN 978-80-8094-958-7. - p. 71-75. (in Slovak)

[15] GALLO, O. - NEČAS, T. - JUHÁS, G.: Synthesis of Asynchronous Digital Circuits with Using Petri Nets. In: SMART S2AI: Workshop of SMART Systems and Services in Applied Informatics. Bratislava, Slovak Republic, 18 April 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3513-1. - p. 6-8. (in Slovak)

[16] HAMBALÍK, A.: Communication Networks and Communication Protocols. In: Trends in Education: Olomouc, Czech Republic, 23-24 June 2011. - Olomouc: Gevak Ltd., 2011. - ISBN 978-80-86768-34-2. - p. 280-283. (in Slovak)

[17] HAMBALÍK, A.: The Examination of the Authenticity of Digital Pictures. In: Agria Media 2011: International Conference on Information. October 11-12, 2011. - Eger: Eszterházy Károly Föiskola, 2011. - p. 32. (in Hungarian)

[18] HÄUPTLE, P. - HUBINSKÝ, P. - RUDOLF, B. - GRUHLER, G.: Signal Types Investigation for Harmonic Modulation in Drives. In: WCECS 2011: Proceedings of the World Congress on Engineering and Computer Science 2010. Volume I. San Francisco, USA, 19-21 October, 2011. - Hong Kong: International Association of Engineers, 2011. - ISBN 978-988-19251-7-6. - p. 951-955. (in English)

[19] HROMADA, V. - VOJVODA, M.: Fault Analysis of Stream Ciphers. In: Santa's Crypto Get-Together 2011: Prague, Czech Republic, 1-2 December 2011. - Prague: Trusted Network Solutions, 2011. - p. 69-70. (in English)

[20] HROMADA, V. - VOJVODA, M.: Fault Analysis of Stream Ciphers. In: ŠVOČ 2011: Proceedings of Selected Works. Bratislava, Slovak Republic, 4. 5. 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3508-7. - p. 25-29. (in Slovak)

[21] JÓKAY, M. - ZAJAC, P.: Analysis of Data Structures in MP4 Files Usable for Steganography. In: ISCAMI 2011: Book of Abstracts. Malenovice, Czech Republic, 6.-8. 5. 2011. - Ostrava: University of Ostrava, 2011. - p. 34. (in English)

[22] JÓKAY, M. - PLANČÍK, M. - ZAJAC, P.: Remarks on GPU Usage in Cryptanalysis. In: GCCP 2011 Proceedings: 7th International Workshop on Grid Computing for Complex Problems. Bratislava, Slovak Republic, October 24 - 26, 2011. - Bratislava: Slovak Academy of Sciences, 2011. - ISBN 978-80-970145-5-1. - p. 78-85. (in English)

[23] JÓKAY, M.: The Design of a Steganographic System Based on the GOP Structure in the Video Standard MPEG-4. In: Recent Researches in Computers and Computing: International Conference on Computers and Computing (ICCC'11). Lanzarote, Spain, 27.-29. 5. 2011. - WSEAS Press, 2011. - ISBN 978-1-61804-000-8. - p. 95-99. (in English)

[24] JUHÁS, G. - FOLTIN, M. - ŠEVČÍKOVÁ, Z. - JUHÁSOVÁ, A.: Could over. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 17, Special Issue: ELOSYS, Trenčín, 11. -14. 10. 2011, p. 204-207. (in Slovak)

[25] KAZLOV, I. - JUHÁS, G.: Introduction to Resource Constrained Workflow Nets. In: SMART S2AI: Workshop of SMART Systems and Services in Applied Informatics. Bratislava, Slovak Republic, 18 April 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3513-1. - p. 14-16. (in Slovak)

[26] KEČKEMÉTYOVÁ, M. - BOCK, I.: An Optimal Control Problem for an Elastic Beam in a Dynamic Contact with a Rigid Obstacle. In: 8th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control: Nemecká, Slovak Republic, September 5-10, 2011. - Bratislava: FEI STU, 2011. - p. 20-25. (in English)

[27] KEČKEMÉTYOVÁ, M. - ROZBOROVÁ, V.: on an Optimal Design Problem for a Mindlin-Timoshenko Beam on a Unilateral Elastic Foundation. In: New Trends in Statics and Dynamics of Buildings: 9th International Conference. Bratislava, Slovak Republic, 20.-21. 10. 2011. - Bratislava: STU, 2011. - ISBN 978-80-227-3572-8. - p. 213-216. (in English)

[28] KOVÁČ, M. - LEHOCKI, F.: Mobile Solution for Chronic Disease Management. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 17, Special Issue: ELOSYS, Trenčín, 11.-14. 10. 2011, p. 208-210. (in Slovak)

[29] LEHOCKI, F. - ORAVEC, M. - BALOGH, Š. - JUHÁSOVÁ, A.: Selected Models for Diagnostic Systems. In: SMART S2AI: Workshop of SMART Systems and Services in Applied Informatics. Bratislava, Slovak Republic, 18 April 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3513-1. - p. 1-5. (in Slovak)

[30] LODERER, M. - REPKA, M.: Cache Collision Time Attack Against AES Using Final Round. In: ŠVOČ 2011: Proceedings of Selected Works. Bratislava, Slovak Republic, 4. 5. 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3508-7. - p. 20-24. (in Slovak)

[31] MARČEK, S. - DROZDA, M. - JUHÁS, G.: Introduction to Intrusion Detection System for High Dimensional Stace for WSN. In: SMART S2AI: Workshop of SMART Systems and Services in Applied Informatics. Bratislava, Slovak Republic, 18 April 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3513-1. - p. 17-18. (in English)

[32] MARKO, Ľ.: Bifurcation Problem for Elastic Circular Plate. In: New Trends in Statics and Dynamics of Buildings: 9th International Conference. Bratislava, Slovak Republic, 20.-21. 10. 2011. - Bratislava: STU, 2011. - ISBN 978-80-227-3572-8. - p. 91-92. (in English)

[33] MARKO, T. - ADAMKO, L.: Extraction of Delta Points from Palmprints. In: ŠVOČ 2011: Proceedings of Selected Works. Bratislava, Slovak Republic, 4. 5. 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3508-7. - p. 15-19. (in Slovak)

[34] MAZANEC, J.: Designing a Complex Face Recognition System. In: ELITECH´11: 13th Conference of Doctoral Students, Faculty of Electrical Engineering and Information Technology. Bratislava, Slovak Republic, 17 May, 2011. - Bratislava: Nakladateľstvo STU, 2011. - ISBN 978-80-227-3500-1. - p. 1-5. (in English)

[35] MAZANEC, J. - ORAVEC, M.: Face Recognition System Based on LBP. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 17, Special Issue: ELOSYS, Trenčín, 11.-14. 10. 2011, p. 217-221. (in Slovak)

[36] NÁNÁSIOVÁ, O. - PASTUCHOVÁ, E. - VÁCLAVÍKOVÁ, Š. - SABO, M.: Classification of Association Coefficients and its Application in Cluster Analysis. In: ODAM 2011: Olomoucian Days of Applied Mathematics. Book of Abstracts. Olomouc, Czech Republic, January 26-28, 2011. - Olomouc: Palacký University, 2011. - ISBN 978-80-244-2684-6. - p. 47. (in English)

[37] OMELINA, Ľ. - ORAVEC, M.: Efficient Face Expression Generation for Face Recognition. In: Proceedings ELMAR-2011: 53rd International Symposium. 14-16 September 2011, Zadar, Croatia. - Zadar: Croatian Society Electronics in Marine, 2011. - ISBN 978-953-7044-12-1. - p. 29-32. (in English)

[38] OMELINA, Ľ.: Face Recognition from Single Sample. In: ICVSS 2011. Registration, Recognition and Reconstruction in Image and Video: International Computer Vision Summer School 2011. Sicily, 11-16 July, 2011. - University of Catania, 2011. - p. 56. (in English)

[39] OMELINA, Ľ. - ORAVEC, M.: Universal Biometric Evaluation System. In: IWSSIP 2011: 18th International Conference on Systems, Signals & Image Processing. Sarajevo, Bosnia and Herzegovina, 16-18 June 2011. - IEEE eXpress, 2011. - ISBN 978-9958-9966-3-4. - p. 307-310. (in English)

[40] PILKA, F. - ORAVEC, M.: Multi-Step Ahead Prediction Using Neural Networks. In: Proceedings ELMAR-2011: 53rd International Symposium. 14-16 September 2011, Zadar, Croatia. - Zadar: Croatian Society Electronics in Marine, 2011. - ISBN 978-953-7044-12-1. - p. 269-272. (in English)

[41] POLAKOVIČ, M.: Some Remarks on Operator Generalized Effect Algebras. In: 8th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control: Nemecká, Slovak Republic, September 5-10, 2011. - Bratislava: STU, 2011. - p. 41-43. (in English)

[42] RACKO, J. - MIKOLÁŠEK, M. - GRMANOVÁ, A. - BREZA, J. - BENKO, P. - GALLO, O. - HARMATHA, L.: a New Model of Multiphon Excitation Trap-Assisted Band-to-Band Tunneling. In: EDS´11. Electronic Devices and Systems IMAPS CS International Conference 2011: Brno, Czech Republic, June 22-23, 2011. - Brno: VUT, 2011. - ISBN 978-80-214-4303-7. - p. 168-174. (in English)

[43] REPKA, M.: DPA of an Aes Implementation. In: ELITECH´11: 13th Conference of Doctoral Students Faculty of Electrical Engineering and Information Technology. Bratislava, Slovak Republic, 17 May, 2011. - Bratislava: Nakladateľstvo STU, 2011. - ISBN 978-80-227-3500-1. - p. 1-6. (in English)

[44] RUDOLF, B.: on Multiple Solutions of Generalized Second Order Boundary Value Problem with ph-Laplacian. In: 8th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control: Nemecká, Slovak Republic, September 5-10, 2011. - Bratislava: STU, 2011. - p. 45-49. (in English)

[45] SABO, M. - NÁNÁSIOVÁ, O. - PASTUCHOVÁ, E. - VÁCLAVÍKOVÁ, Š.: Comparing Similarities in Cluster Analysis. In: ISCAMI 2011: Book of Abstracts. Malenovice, Czech Republic, 6.-8. 5. 2011. - Ostrava: University of Ostrava, 2011. - p. 60. (in English)

[46] STRAČÁR, P. - SLAMKA, M. - ORAVEC, M. - PAVLOVIČOVÁ, J.: Kernel and Linear Methods for Biometric Face Recognition. In: IN-TECH 2011: Proceedings of International Conference on Innovative Technologies. Bratislava, Slovak Republic, 1. 9. -3. 9. 2011. - Jaroměř: Jan Kudláček, 2011. - ISBN 978-80-904502-6-4. - p. 524-527. (in English)

[47] ŠEVČÍKOVÁ, Z. - JUHÁS, G.: Application of Petri Nets in Smart Systems. In: SMART S2AI: Workshop of SMART Systems and Services in Applied Informatics. Bratislava, Slovak Republic, 18 April 2011. - Bratislava: FEI STU, 2011. - ISBN 978-80-227-3513-1. - p. 9-10. (in Slovak)

[48] ŠEVČÍKOVÁ, Z. - KAZLOV, I. - JUHÁSOVÁ, A.: Possibility of Using Analysis and Synthesis of Event Systems in Practice. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 17, Special Issue: ELOSYS, Trenčín, 11.-14. 10. 2011, p. 227-229. (in Slovak)

[49] VÁLKY, G. - LEHOCKI, F. - KOVÁČ, M.: Wireless System for Online Acquisition of ECG Waveforms of Human Heart. In: AMA-IEEE Medical Technology Conference: Healthcare IT: 2nd AMA-IEEE Medical Technology Conference on Delivering on the Promise of Cost Effective Quality Healthcare. Boston, Massachusetts, 16-18 October 2011. - Piscataway: IEEE, 2011. - CD-Rom. (in English)

[50] ZAJAC, M.: Examples of Non-Hyperreflexive Reflexive Spaces of Operators. In: 8th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control: Nemecká, Slovak Republic, September 5-10, 2011. - Bratislava: FEI STU, 2011. - p. 56-59. (in English)

[51] ZAJAC, M.: Unbounded Linear Operator in Effect Algebras. In: Quantum Structures 2011: 3rd International Conference. Kočovce, Slovak Republic, 16.-20. 5. 2011. - Bratislava: STU, 2011. - ISBN 978-80-227-3515-5. (in English)

[52] ZAJAC, P. - ČAGALA, R.: Algebraic Cryptanalysis of the Block Cipher Gost. In: 11th Central European Conference on Cryptology: Debrecen, Hungary, 30 June - 2 July, 2011. - Debrecen: University of Debrecen, 2011. - p. 1. (in English)

[53] ZÁKOPČAN, M.: a Note on One-Dimensional Macroelectronic Model in Problem of Linear-Quadratic Approximation in RBC Models. In: Acta Mathematica 14: Nitra, Slovak Republic, 22.-23. September 2011. - Nitra: Constantine the Philosopher University in Nitra, 2011. - ISBN 978-80-8094-958-7. - p. 253-258. (in Slovak)

[54] ZELINA, M. - ORAVEC, M.: Decision Trees for Recognition of Internet Applications. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Vol. 17, Special Issue: ELOSYS, Trenčín, 11.-14. 10. 2011, p. 234-237. (in English)

[55] ZELINA, M. - ORAVEC, M.: Early Detection of Internet Applications. In: Proceedings of 9th International Conference VSACKÝ CÁB 2011. - Brno University of Technology, 2011. - ISBN 978-80-214-4319-8. - p. 157-160. (in English)

[56] ZELINA, M. - ORAVEC, M.: Early Detection of Network Applications Using Neural Networks. In: Proceedings ELMAR-2011: 53rd International Symposium. 14-16 September 2011, Zadar, Croatia. - Zadar: Croatian Society Electronics in Marine, 2011. - ISBN 978-953-7044-12-1. - p. 161-164. (in English)

[57] ŽILKA, T. - PANCZA, D.: a Viscoelastic Membrane in a Dynamic Contact with a Rigid Obstacle. In: New Trends in Statics and Dynamics of Buildings: 9th International Conference. Bratislava, Slovak Republic, 20.-21. 10. 2011. - Bratislava: STU, 2011. - ISBN 978-80-227-3572-8. - p. 217-220. (in English)

## IX. 3 Books

[1] JUHÁS, G.: Algebraically Generalised Petri Nets. - Bratislava: RT Systems, 2011. - 185 p. - ISBN 978-80-970519-3-8. (in English)

[2] JUHÁS, G.: Are These Events Independent? It Depends!. - Bratislava: RT Systems, 2011. - 145 p. - ISBN 978-80-970519-2-1. (in English)

[3] JUHÁS, G.: Modelling Formalisms of Event Systems. - Bratislava: RT Systems, 2011. - 112 p. - ISBN 978-80970519-1-4. (in Slovak)

## IX. 4 Parts of Books

[1] BRILLA, I.: Numerical Solution of Boundary Inverse Problem for Anisotropic Solids. In: Solid Mechanics in Brazil 2011. - Rio de Janeiro: Brazilian Society of Mechanical Sciences and Engineering, 2011. - ISBN 978-85-85769-46-8. - p. 77-88. (in English)

[2] HUBINSKÝ, P. - RUDOLF, B. - HÄUPTLE, P.: Optimization of the Signal-Type Used in a Harmonic Modulator for Control. In: Selected Topics in Modelling and Control. Vol. 7. - Bratislava: Slovak University of Technology, 2011. - ISBN 978-80-227-3597-1. - p. 118-123. (in English)

[3] MARKO, Ľ.: Calculus on-line. In: Theoretical and Educational Transformation of Mathematical Education 2011: Proceedings of Scientific Papers. - Nitra: Slovak University of Agriculture in Nitra, 2011. - ISBN 978-80-552-0604-2. - p. 93-98. (in Slovak)

[4] ORAVEC, M. - PAVLOVIČOVÁ, J. - MAZANEC, J. - OMELINA, Ľ. - FÉDER, M. - BAN, J.: Efficiency of Recognition Methods for Single Sample per Person Based Face Recognition. In: Reviews, Refinements and New Ideas in Face Recognition. - Rijeka: InTech, 2011. - ISBN 978-953-307-368-2. - p. 181-206. (in English)

## IX. 5 Textbooks

[1] KOSTRECOVÁ, E. - JÓKAY, M. - KOSTREC, M.: Computer Crime. - Bratislava: STU in Bratislava, 2011. - 109 p. - ISBN 978-80-227-3410-3. (in Slovak)

STU
FEI

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY
A INFORMATIKY

www.stuba.sk