

# SPRÁVA O VEDECKO-VÝSKUMNEJ ČINNOSTI na Ústave informatiky a matematiky FEI STU v Bratislave

za rok 2016

## riaditeľ ústavu:

prof. RNDr. Otokar Grošek, PhD.  
e-mail: otokar.grosek@stuba.sk

Tel: ++421-2-602 91 226  
Fax: ++421-2-654 20 415

## I. PRACOVNÍCI

### Profesori

prof. RNDr. Igor Bock, PhD.  
prof. RNDr. Otokar Grošek, PhD.  
prof. RNDr. Gabriel Juhás, PhD. (vedúci odd. SI)  
prof. Dr. Ing. Miloš Oravec

### Docenti

Dr. rer. nat. Martin Drozda  
doc. RNDr. Ľubomír Marko, CSc. (vedúci odd. Matematiky)  
doc. RNDr. Karol Nemoga, PhD.  
doc. RNDr. Oľga Nánásiová, PhD.  
doc. RNDr. Vladimír Olejček, PhD.  
doc. Mgr. Marcel Polakovič, PhD.  
doc. RNDr. Boris Rudolf, PhD.  
doc. Ing. Michal Šrámka, PhD., PhD.  
doc. Ing. Milan Vojvoda, PhD.  
doc. RNDr. Michal Zajac, PhD.  
doc. Ing. Pavol Zajac, PhD. (vedúci odd.BIS)

### Odborní asistenti

Ing. Štefan Balogh, PhD.  
RNDr. Igor Brilla, PhD.  
RNDr. Viera Čerňanová, PhD.  
RNDr. Karla Čipková, PhD.  
Ing. Ondrej Gallo, PhD.  
Ing. Alexander Hambalík, PhD.  
Ing. Viliam Hromada, PhD.  
Ing. Mgr. Matúš Jókay, PhD.  
RNDr. Mária Kečkemétyová, PhD.  
RNDr. Igor Kossaczky, CSc.  
Ing. Stanislav Marček, PhD.  
RNDr. Ivica Marinová, PhD.  
Ing. Vladislav Novák  
Mgr. Dávid Pancza, PhD.  
RNDr. Elena Pastuchová, PhD.  
Mgr. Marek Sýs, PhD.  
Mgr. Zuzana Ševčíková  
Mgr. Michal Zákopčan, PhD.

**Administratívni pracovníci** Zuzana Šabíková (tajomníčka ústavu)  
Emília Komžíková  
Mgr. Zuzana Šedová

**Interní doktorandi** Ing. Eugen Antal  
Ing. Maroš Čavojský  
Mgr. Tomáš Fabšič  
Ing. Michala Gulášová  
Ing. Vojtěch Jirka (prerušené od 1.7.2015)  
Ing. Pavol Marák  
Ing. Ľuboš Omelina (ukončil 14.11.2016)  
Ing. Alexandra Posoldová (zanechala k 31.8.2016)  
Ing. Dominik Sopiak  
Ing. Juraj Varga

**Externí doktorandi** Ing. Robert Bučko  
Ing. Csaba Cserba  
Ing. Igor Kazlov  
Mgr. Jozef M. Kollár (ukončil 21.11.2016)  
MUDr. Veronika Kurilová (prerušené do 2.9.2018)  
Ing. Stanislav Marček (ukončil 31.8.2016)  
Ing. Peter Minarovský  
Ing. Štefan Počarovský (prerušené do 31.5.2018)  
Mgr. Zuzana Ševčíková (zanechala k 1.9.2016)  
Mgr. Tomáš Žilka  
Mgr. Viktória Žilková (rod.Rozborová)

## II. ZARIADENIA

### II.1. Výukové a výskumné laboratóriá

- Laboratórium Biometrie a spracovania signálov
- Laboratórium pre Bezpečnosť IT
- Laboratórium pre databázy - DIEDC (Database Information Education and Demonstration Center)
- Laboratórium Komunikačných sietí
- Antivírusové laboratórium
- Experimentálne laboratórium ÚIM
- Knižnica Oddelenia matematiky ÚIM
- Časopisecká knižnica Oddelenia matematiky ÚIM

### LAB: Mobile Computing & Petri Net Lounge (ešte vo výstavbe)

Výkonné počítače:

- CPU 4-jadrový Intel Xeon E5-1620v3/RAM 256GB/SSD 256GB RAID0/HDD 2TB RAID5
- CPU 8-jadrový AMD FX-9590/RAM 32GB/SSD 256GB/ HDD 3TB/GPU 2x NVIDIA GTX970 v SLI
- CPU 4-jadrový Intel i7-4790/RAM16GB/SSD 256GB/ HDD 1TB Raid1

## II.2. Špeciálne meracie zariadenia, počítače a vybavenie

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

## III. VÝUČBA

### III.1. Bakalárske štúdium (Bc.)

●Algebraické štruktúry (B-AS)	(6. sem 2-2 h)	O. Nánásiová/ D. Pancza M. Vojvoda
●Analýza a zložitosť algoritmov (B-AZA)	(5. sem. 3-1 h)	M. Vojvoda
●Databázové systémy (B-DBS)	(4. sem. 2-2 h)	M. Polakovič/ V. Čerňanová/ K. Čipková
●Diskrétna matematika (B-DM)	(4. sem .2-2 h)	G.Juhás
●Diskrétné udalostné systémy (B-DUS)	(3. sem. 2-2 h)	O. Grošek/ A. Hambalík
●História informatiky (B-HI)	(4. sem. 2-1 h)	O. Grošek
●Klasické šifry (B-KSIF)	(5. sem. 2-2 h)	
●Lineárna algebra (B-LA)	(3. sem. 2-2 h)	M. Zajac/ I. Marinová/ O. Nánásiová
●Matematická analýza 1 (MA1_B FIIT)	(1. sem. 4-2 h)	Ľ. Marko/ M. Zákopčan
●Matematická štatistika (B-MATSTAT)	(4. sem. 3-2 h)	O.Nánásiová/ I. Marinová/ E.Pastuchová
●Matematika 1 (B-MAT1E)	(1. sem. 3-2 h)	M. Zajac/ M.Zákopčan/ V.Čerňanová
●Matematika 1 (B-MAT1I)	(1. sem. 3-2 h)	B. Rudolf/ M.Polakovič/ E.Pastuchová/ M. Kečkemétyová
●Matematika 1 op. (B-MAT1I)	(2. sem. 3-2 h)	I. Bock
●Matematika 1 op. (B-MAT1E)	(2. sem. 3-2 h)	V. Olejček
●Matematika 2 (B-MAT2E)	(2. sem. 3-2 h)	Ľ. Marko/ I.Brilla
●Matematika 2 (B-MAT2I)	(2. sem. 3-2 h)	B. Rudolf/ M. Zákopčan/ M. Kečkemétyová
●Matematika 2 op. (B-MAT2I, B-MAT2E)	(3. sem. 3-2 h)	V. Olejček/

●Matematika 3 (B-MAT3)	(3. sem. 3-2 h)	Ľ. Marko I.Brilla
●Matematika 4 (B-MAT4)	(4. sem. 3-2 h)	V. Olejček
●Objektovo orientované programovanie (B-OOP)	(3. sem. 2-2 h)	G. Juhás
●Operačné systémy (B-OS)	(5. sem. 2-2 h)	M. Šrámka/ M. Jókay
●Obyčajné diferenciálne rovnice (B-ODR-Stav.f)	(3. sem. 2-2 h)	I. Bock
●Počítačová kriminalita (B-PKRIM)	(6. sem. 2-2 h)	Š. Balogh
●Počítačové siete (B-PS)	(3. sem. 2-2 h)	M.Oravec
●Pravdepodobnosť a štatistika (PAS_B)	(6. sem. 2-2 h)	V. Olejček
●Programovacie techniky (B-PT)	(3. sem. 3-2 h)	M. Drozda
●Rýchle algoritmy (B-RAL)	(6. sem. 2-2 h)	K. Nemoga/ K. Čipková
●Seminár z B-MAT1I	(1. sem. 0-2 h)	B. Rudolf/ M. Kečkemétyová/
●Seminár z B-MAT1E	(1. sem. 0-2 h)	M. Zajac
●Seminár z B-MAT2I	(2. sem. 0-2 h)	B. Rudolf
●Seminár z B-MAT2E	(2. sem. 0-2 h)	Ľ. Marko
●Softvérové inžinierstvo (B-SWI)	(5. sem. 2-2 h)	M. Šrámka
●Vývoj softvérových aplikácií (B-VSA)	(6. sem. 2-2 h)	G. Juhás/ I. Kossaczky

### III.2. Inžinierske štúdium (Ing.)

●Algoritmy a dátové štruktúry (I-ADS)	(3. sem. 3-2 h)	M. Vojvoda
●Architektúra softvérových systémov (I-ASOS)	(3. sem. 2-2 h)	G. Juhás/ I. Kossaczky
●Automaty a formálne jazyky (I-AFJ)	(2. sem. 2-2 h)	O. Grošek/ V. Hromada
●Bezpečnosť informačných systémov s pohľadom praxe (I-BISPP)	(2. sem. 3-2 h)	M. Šrámka
●Kódovanie (KOD_I) - FIIT	(1. sem. 2-2 h)	K. Čipková
●Logika (I-LOG)	(1.+3. sem. 3-2 h)	K. Nemoga/ K. Čipková
●Matematika (I-MAT)	(1. sem. 2-2 h)	I. Bock
●Mobilné výpočty (I-MOBV)	(3. sem. 2-2 h)	M. Drozda
●Modelovanie a simulácia udalostných systémov (I-MSUS)	(1. sem. 2-2 h)	G. Juhás
●Návrh a kryptoanalýza šifrier (I-NKS)	(3. sem. 2-2 h)	P.Zajac
●Paralelné programovanie a distribuované systémy (I-PPDS)	(3. sem. 2-2 h)	M. Drozda/ M. Jókay
●Reprezentácia a získavanie znalostí (I-RZZ)	(1.+3. sem. 2-2 h)	K. Nemoga/ I. Kossaczky
●Spoločenské, morálne a právne súvislosti vývoja informačných systémov (I-SMPSVIS)	(3. sem. 3-0 h)	M. Šrámka
●Strojové učenie a neurónové siete (I-SUNS)	(1. sem. 2-2 h)	M. Oravec
●Šifrovanie v komunikačných sieťach (I-SKS)	(1. sem. 3-2 h)	K. Nemoga/ M. Sýs
●Úvod do počítačovej bezpečnosti (I-UPB)	(1. sem. 2-1 h)	P. Zajac
●Základy kryptografie (I-ZKRY)	(1. sem. 2-2 h)	O. Grošek

### III.3. Doktorandské štúdium (PhD.)

- |   |            |
|---|------------|
| •Matematika pre doktorandov                                 | I. Bock    |
| •Predmet špecializácie Aplikovaná informatika II            | M. Oravec  |
| •Teoretické princípy informačných vied- Stochastické modely | V. Olejček |
| •Teória odboru Aplikovaná informatika                       | M. Oravec  |

### III.4. Bakalárske a inžinierske štúdium pre zahraničných študentov (v anglickom jazyku)

- |  |              |
|--|--------------|
| •Algoritmizácia a programovanie                  | V. Hromada   |
| •Analýza a zložitosť algoritmov                  | M. Vojvoda   |
| •Architektúra počítačov                          | M. Jókay     |
| •Databázové systémy                              | M. Vojvoda   |
| •Diskrétna matematika                            | O. Nánásiová |
| •História informatiky                            | O. Grošek    |
| •Klasické šifry                                  | O. Grošek    |
| •Matematika 1                                    | M. Zajac     |
| •Matematika 2                                    | K. Čipková   |
| •Matematika 3                                    | Ľ. Marko     |
| •Matematická štatistika                          | O. Grošek    |
| •Lineárna algebra                                | M. Zajac     |
| •Objektovo-orientované programovanie             | I. Kazlov    |
| •Operačné systémy                                | M. Jókay     |
| •Paralelné programovanie a distribuované systémy | M. Jókay     |
| •Počítačové siete                                | J. Varga     |
| •Softvérové inžinierstvo                         | M. Šrámka    |
| •Úvod do inžinierstva                            | T. Fabšič    |

### III.5. Dištančné štúdium

- |                   |                        |          |
|-------------------|------------------------|----------|
| •Matematika 3     | (3. sem. 6x2h konzul.) | Ľ. Marko |
| •Lineárna algebra | (3. sem. 6x2h konzul.) | M. Zajac |

## IV. VÝSKUMNÉ PROJEKTY

### IV.1. Projekty VEGA, ESF, APVV a iné riešené v roku 2016 na ÚIM

**Číslo projektu:** VEGA 1/0529/13

**Názov projektu:** Návrh pokročilých metód biometrického rozpoznávania na základe obrazov tváre a dúhovky

**Zodpovedný riešiteľ:** prof. Dr. Ing. Miloš Oravec

**Spoluriešitelia z ÚIM v roku 2016:** Mgr. Ing. Matúš Jókay, PhD., doc. Ing. Milan Vojvoda, PhD., Ing. Marek Sýs, PhD.

**Doba riešenia:** 2013 - 2016

## **IV.2. Výskumné úlohy**

### **IV.2.1. Program na podporu mladých výskumníkov**

### **IV.2.2 Pokračujúce projekty na podporu excelentných mladých výskumníkov**

## **IV.3. Zahraničné projekty**

**Číslo projektu:** NATO: SfP 984520

**Názov projektu:** Secure Implementation of Post-Quantum Cryptography

**Riaditeľ projektu:** prof. RNDr. Otokar Grošek, PhD.

**Spoluriešitelia zo SR na ÚIM v roku 2016:** doc. Ing. Pavol Zajac, PhD., Ing. Marek Repka, Ing. Ondrej Gallo, PhD., Ing. Juraj Varga, Ing. Eugen Antal, Ing. Viliam Hromada, PhD., Mgr. Tomáš Fabšič, doc. RNDr. Karol Nemoga, PhD.

**Doba riešenia:** 2012-2016

### **IV.3.1. Bilaterálna spolupráca**

**Názov projektu:** SECOSYS – Security and privacy in mobile computing ecosystems

**Číslo projektu:** DAAD

**Zodpovedný riešiteľ:** Dr. rer. nat. Martin Drozda

**Riešitelia z ÚIM v roku 2016:** doc. Ing. Pavol Zajac, PhD., Ing. Štefan Balogh, PhD., Ing. Juraj Varga, Ing. Stanislav Marček, Ing. Maroš Čavojský

**Trvanie projektu:** 2015-2016

**Názov projektu:** Kryptografia prináša bezpečnosť a slobodu

**Číslo projektu:** SK06-IV-01-001

**Zahraničný partner:** Selmenovo centrum, Institutt for Informatikk, Universitetet i Bergen, Nórsko

**Vedúci projektu:** prof. RNDr. Otokar Grošek, PhD.

**Vedúci za nórsku stranu:** Tor Helleseth

**Riešitelia z ÚIM v roku 2016:** doc. RNDr. Karol Nemoga, PhD., doc. Ing. Milan Vojvoda, PhD., doc. Ing. Pavol Zajac, PhD., Mgr. Ing. Matúš Jókay, PhD., Ing. Eugen Antal, Ing. Juraj Varga, Ing. Viliam Hromada, PhD., Ing. Pavol Marák, Mgr. Tomáš Fabšič

**Riešitelia z Nórska:** Igor Semaev, Lilya Budaghyan, Seyed M. M. H. Zadeh, Oleksandr Kholosha, Håvard Raddum

**Trvanie projektu:** 10.4.2015-31.3.2016

## **IV.4. Zapojenie členov ÚIM do výskumných projektov mimo ÚIM**

**Číslo projektu:** APVV-0246-12

**Názov projektu:** Pokročilé metódy modelovania a simulácie SMART mechatronických systémov

**Vedúci projektu:** prof. Ing. Justín Murín, DrSc., ÚAM FEI STU

**Spoluriešiteľ z ÚIM v roku 2016:** prof. RNDr. Igor Bock, PhD.

**Doba riešenia:** 01.10.2013-30.09.2016

**Číslo projektu:** APVV-15-0326

**Názov projektu:** Smart mestá a ich inteligentná energetická chrbtica

**Vedúci projektu:** prof. Ing. František Janíček, PhD., ÚEAE FEI STU

**Spoluriešiteľ z ÚIM v roku 2016:** RNDr. Igor Brilla, PhD.

**Doba riešenia:** 01.07.2016-30.09.2019

## **V. SPOLUPRÁCA**

### **V.1. Domáca spolupráca**

#### **V.1.1. Pozvané prednášky**

**Meno:**

**Príspevok:**

#### **V.1.2. Spolupráca s domácimi inštitúciami**

- Národný bezpečnostný úrad SR, Bratislava
- Kriminologický a expertízny ústav Policajného zboru MV SR, Bratislava
- Univerzita J. Selyeho v Komárne
- Metodicko-pedagogické centrum mesta Bratislavy
- Virtuálna akadémia bratislavského samosprávneho kraja
- Agentúra na podporu výskumu a vývoja, Bratislava
- Matematický ústav SAV, Bratislava
- Stredisko dištančného vzdelávania (SDV ICV CUP REK) záverečné práce
- Centire s. r. o., Záhradnícka 72, Bratislava – projekt e-Academy pre Daňové riaditeľstvo SR
- Ministerstvo financií SR, Národná koncepcia informatizácie verejnej správy
- Ústav merania SAV, Bratislava
- Slovenský ústav technickej normalizácie, Bratislava
- Ministerstvo zdravotníctva SR, Strategické ciele eHealth
- Národné centrum zdravotníckych informácií, Bratislava, eHealth
- Fakulta manažmentu, UK, Bratislava
- ÚIAa M FCHPT STU ( prof. Kolesárová, doc. Šabo)
- Katedra matematiky a deskriptívnej geometrie SvF STU (prof. Mesiar, prof. Širáň, prof. Komorníková, prof. Mikula, doc. Kalina, doc. Jenča)
- Katedra matematickej analýzy FMFI UK (doc.Kubáček)
- Katedra matematiky AOS Liptovský Mikuláš (doc. Chovanec, doc. Jurečková, dr. Drobná)
- Katedra matematiky SjF STU ( doc.Velichová, dr. Kováčová, doc. Dobrákovová)
- IBM Slovensko, s.r.o.
- WHO kancelária na Slovensku (MUDr. Darina Sedláková)
- Ministerstvo obrany SR

### **V1.3. Pozvané prednášky domácich odborníkov**

**Host' (adresa):**

**Termíny:**

**Účel:**

**Prednáška:**

## **V.2. Zahraničná spolupráca**

### **V.2.1. Pozvané prednášky**

**Meno: doc. Ing. Pavol Zajac, PhD.**

**Miesto:** Oslo, Nórsko

**Prednáška:** Side-channel attacks

**Dátum:** 13.-15.4.2016

**Meno: prof. RNDr. Gabriel Juhás, PhD.**

**Miesto:** Hamilton, Kanada

**Dátum:** 19.-26.3.2016

### **V.2.2. Spolupráca so zahraničnými inštitúciami**

- MINT, Emmy Noether Verein, Ulm, Germany (prof. Gudrun Kalmbachová).
- Institut für Algebra und Computermathematik TU, Vienna, Austria (prof. Dietmar Dorninger)
- Math.Institute, Polish Academy of Sciences, Warsaw, Poland (prof. Jaroslav Zemánek)
- University of Ljubljana, Ljubljana, Slovenia (doc. J.Bračič).
- Institut de Mathematiques, Université Louis Pasteur, Strasbourg, France (prof. Vilmos Komornik)
- Eszterházy Károly Főiskola, Eger, Maďarsko (Dr. Kis Tóth Lajos, Tóthné dr. Parázsó Lenke)
- Matematický ústav AVČR (RNDr. Jiří Jarušek, DrSc., doc. RNDr. Vladimír Müller, DrSc., RNDr. Miroslav Šilhavý DrSc.)
- Ústav informatiky AVČR (prof. RNDr. Štefan Porubský, DrSc.).
- School of Computer Science, Tel Aviv Univerzity, Tel Aviv, Israel (Dr. Eran Tromer)
- Hubert Curien Laboratory, Jean Monnet University, Saint-Étienne, France (Prof. Viktor Fischer)
- Department of Mathematical Sciences, Florida Atlantic University, Boca Raton, FL, USA (Dr. Rainer Steinwandt)
- Přírodovědecká fakulta Univerzity Hradec Králové, Česká republika
- FernUniversität in Hagen (prof. Dr. Desel)
- University of Houston, Department of Biomedical Engineering, USA (prof. Metin Akay)



### **V.2.3. Zahraniční hostia**

**Host' (adresa):**

**Termín:**

**Účel:**

**Prednáška:**

### **V.2.4. Pobyty pracovníkov ÚIM v zahraničí**

**Meno: doc. Ing. Pavol Zajac, PhD.**

**Miesto:** Bergen, Nórsko

**Účel:** účasť na workshope k projektu EHP SK06-IV-01001

**Dátum:** 6.-11.2.2016

**Meno: Ing. Viliam Hromada, PhD.**

**Miesto:** Bergen, Nórsko

**Účel:** účasť na workshope k projektu EHP SK06-IV-01001

**Dátum:** 6.-11.2.2016

**Meno: Ing. Onderj Gallo, PhD.**

**Miesto:** Bergen, Nórsko

**Účel:** účasť na workshope k projektu EHP SK06-IV-01001

**Dátum:** 6.-11.2.2016

**Meno: doc. Ing. Michal Šrámka, PhD.**

**Miesto:** Bergen, Nórsko

**Účel:** účasť na workshope k projektu EHP SK06-IV-01001

**Dátum:** 6.-11.2.2016

**Meno: Ing. Eugen Antal**

**Miesto:** Bergen, Nórsko

**Účel:** účasť na workshope k projektu EHP SK06-IV-01001

**Dátum:** 6.-11.2.2016

**Meno: Mgr. Tomáš Fabšič**

**Miesto:** Bergen, Nórsko

**Účel:** účasť na workshope k projektu EHP SK06-IV-01001

**Dátum:** 6.-11.2.2016

**Meno: Ing. Pavol Marák**

**Miesto:** Bergen, Nórsko

**Účel:** účasť na workshope k projektu EHP SK06-IV-01001

**Dátum:** 6.-11.2.2016

**Meno: Ing. Juraj Varga**

**Miesto:** Bergen, Nórsko

**Účel:** účasť na workshope k projektu EHP SK06-IV-01001

**Dátum:** 6.-11.2.2016

**Meno: Ing. Michala Gulášová**

**Miesto:** Bergen, Nórsko

**Účel:** účasť na workshope k projektu EHP SK06-IV-01001

**Dátum:** 6.-11.2.2016

**Meno: Ing. Viliam Hromada, PhD.**

**Miesto:** Tel-Aviv, Izrael

**Účel:** účasť na workshope k projektu NATO: SfP 984520

**Dátum:** 24. - 29.9.2016

**Meno: Mgr. Tomáš Fabšič**

**Miesto:** Worcester Polytechnic Institute, Worcester, MA, USA

**Účel:** výskum k projektu NATO SPS project 984520

**Dátum:** 19.-24.10.2016

**Meno: Ing. Ondrej Gallo, PhD.**

**Miesto:** Worcester Polytechnic Institute, Worcester, MA, USA

**Účel:** výskum k projektu NATO SPS project 984520

**Dátum:** 19.-24.10.2016

**Meno: Mgr. Tomáš Fabšič**

**Miesto:** Barcelona, Španielsko

**Účel:** účasť na škole pre doktorandov a mladých výskumníkov "COST-IACR School on Randomness in Cryptography"

**Dátum:** 14.-18.11.2016

#### **V.2.5. Zahranické cesty**

**Meno: prof. RNDr. Gabriel Juhás, PhD.**

**Miesto:** Hamilton, Kanada

**Zámer cesty:** účasť na obhajobe ako oponent

**Dátum:** 19.-26.3.2016

**Meno: prof. RNDr. Otokar Grošek, PhD.**

**Miesto:** Brusel, Belgicko

**Zámer cesty:** účasť na obhajobe Ing. L. Omelinu ako podpredseda komisie

**Dátum:** 13.-14.11.2016

**Meno: prof. Dr. Ing. Miloš Oravec**

**Miesto:** Brusel, Belgicko

**Zámer cesty:** účasť na obhajobe Ing. L. Omelinu ako člen komisie

**Dátum:** 13.-14.11.2016

#### **V.2.6. Stáže zahraničných pracovníkov na ÚIM FEI STU**

### V.3. Členstvo v medzinárodných organizáciách a spoločnostiach<sup>1</sup>

- **prof. RNDr. Igor Bock, PhD.** je členom ISSMO a GAMM
- **RNDr. Igor Brilla, PhD.** je členom ISIMM a IACM
- **Dr.rer.nat. Martin Drozda** je členom ACM SIGMOBILE.
- **prof. RNDr. Otokar Grošek, PhD.** je zástupcom SR v European Cooperation in the field of Scientific and Technical Research (COST) Action IC1306: Cryptography for Secure Digital Interaction.
- **RNDr. Ivica Marinová, PhD.** je členkou ENS v Nemecku
- **doc. RNDr. Ľubomír Marko, PhD.** je členom IACM a SIAM
- **doc. RNDr. Karol Nemoga, PhD.** je členom IACR a SIAM
- **doc. RNDr. Vladimír Olejček, PhD.** je členom IQSA, člen Bernoulli's Society, SIAM a AMS
- **prof. Dr. Ing. Miloš Oravec** je členom IEEE IET
- **RNDr. Elena Pastuchová, PhD.** je členkou ENS v Nemecku

## VI. OBHÁJENÉ DIZERTÁCIE

**Ing. Stanislav Marček** – *Využitie kaskádovej klasifikácie pre detekciu chýb, systémových zlyhaní a sieťových prienikov*, školiteľ Dr.rer.nat. Martin Drozda, 31.8.2016

**Ing. Luboš Omelina** – *Visual Human Recognition and identification*, školiteľ prof. Dr. Miloš Oravec, 14.11.2016

**Mgr. Jozef Kollár** - *Štatistická analýza textov pre potreby kryptoanalýzy*, školiteľ prof. RNDr. Otokar Grošek, PhD., 21.11.2016

---

<sup>1</sup> AMS - American Mathematical Society

ISSMO - International Society of Structural and Multidisciplinary Optimization

GAMM - Gesellschaft für Angewandte Mathematik und Mechanik

ISIMM - International Society for the Interaction of Mechanics and Mathematics

IACM - International Association for Computational Mechanics

SIAM - Society for Industrial and Applied Mathematics

IQSA - International Quantum Structures Association

ENS - Emmy Noether Society

IEEE EMBS - The Institute of Electrical and Electronics Engineers, Engineering Medicine & Biology Society

IEEE IET - Institute of Electrical and Electronics Engineers, Institution of Engineering and Technology

IACR - International Association for Cryptologic Research

## VII. INÉ AKTIVITY

### VII.1. Akademické a iné funkcie

- **prof. RNDr. Igor Bock, PhD.** je podpredsedom Odborovej komisie (OK) doktorandského štúdia v študijnom programe 3. stupňa 9.1.9 Aplikovaná matematika so sídlom na SvF STU.
- **prof. RNDr. Igor Bock, PhD.** je garantom externého doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika na FEI STU.
- **prof. RNDr. Igor Bock, PhD.** je členom Odborovej komisie doktorandského štúdia v študijnom programe 3. stupňa 9.1.5 Numerická analýza a vedecko-technické výpočty so sídlom na FMFI UK.
- **prof. RNDr. Otokar Grošek, PhD.** je členom Vedeckej rady FEI STU
- **prof. RNDr. Otokar Grošek, PhD.** je predsedom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na STU
- **prof. RNDr. Otokar Grošek, PhD.** je člen Odborovej komisie (OK) doktorandského štúdia v odbore 9-1-11 Pravdepodobnosť a matematická štatistika na UMB v Banskej Bystrici od r. 2009.
- **Ing. Alexander Hambalík, PhD.** je lektorom Virtuálnej akadémie Bratislavského samosprávneho kraja
- **Ing. Alexander Hambalík, PhD.** je členom odbornej komisie študentskej vedeckej konferencie FTDK v odbore informatika a prírodné vedy – Univerzita J. Selyeho v Komárne
- **Ing. Alexander Hambalík, PhD.** je akreditovaným skúšobným komisárom pre ECDL v Akreditovanom skúšobnom centre č. 062 FEI STU
- **Ing. Alexander Hambalík, PhD.** je členom komisie pre obhajoby záverečných projektov dvojročného špecializovaného kvalifikačného štúdia z informatiky, realizovaného v Metodicko pedagogickom centre Bratislava, Ševčenkova ul.
- **Ing. Alexander Hambalík, PhD.** ELFA, s.r.o. Košice, Datalan, s.r.o. Bratislava, ÚIPŠ MŠ Bratislava, certifikovaný lektor v projekte MVP podporovaný ESF
- **Ing. Mgr. Matúš Jókay, PhD.** je členom AS FEI STU
- **prof. RNDr. Gabriel Juhás, PhD.** je členom OK študijného programu Aplikovaná informatika na STU
- **prof. RNDr. Gabriel Juhás, PhD.** je členom Rady Výskumného centra STU
- **prof. RNDr. Gabriel Juhás, PhD.** je členom riadiaceho výboru pre spoluprácu STU Bratislava a ENEL Slovenské elektrárne, a.s.
- **doc. RNDr. Ľubomír Marko, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU.
- **doc. RNDr. Ľubomír Marko, PhD.** je členom Vedeckej rady FEI STU
- **doc. RNDr. Karol Nemoga, PhD.** je členom Vedeckej rady Matematického ústavu SAV
- **doc. RNDr. Karol Nemoga, PhD.** je podpredseda Edičnej rady SAV
- **doc. RNDr. Karol Nemoga, PhD.** je člen Snemu SAV
- **doc. RNDr. Karol Nemoga, PhD.** je člen NATO ISEG, Brusel
- **doc. RNDr. Karol Nemoga, PhD.** je člen Vedeckej rady Prírodovedeckej fakulty Univerzity Hradec Králové
- **doc. RNDr. Vladimír Olejček, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU.

- **prof. Dr. Ing. Miloš Oravec** je dekanom FEI STU
- **prof. Dr. Ing. Miloš Oravec** je predsedom Vedeckej rady FEI STU
- **prof. Dr. Ing. Miloš Oravec** je predsedom Kolégia dekana FEI STU
- **prof. Dr. Ing. Miloš Oravec** je členom Kolégia rektora STU v Bratislave a členom Vedeckej rady STU v Bratislave
- **prof. Dr. Ing. Miloš Oravec** je členom Vedeckých rád MFF UK, FEI TU v Košiciach, EF ŽU v Žiline, FIIT STU v Bratislave, MTF STU v Bratislave
- **prof. Dr. Ing. Miloš Oravec** je členom OK študijného programu Aplikovaná informatika a členom OK Kybernetika na STU
- **prof. Dr. Ing. Miloš Oravec** je garantom študijného programu bakalárskeho a inžinierskeho štúdia Aplikovaná informatika na FEI STU
- **prof. Dr. Ing. Miloš Oravec** je členom komisie KEGA (Kultúrna a edukačná grantová agentúra Ministerstva školstva, vedy, výskumu a športu SR)
- **doc. RNDr. Boris Rudolf, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU
- **doc. RNDr. Boris Rudolf, PhD.** je členom AS FEI STU (do 30.10.2016)
- **doc. RNDr. Michal Zajac, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU
- **doc. RNDr. Michal Zajac, PhD.** je členom AS FEI STU (od 1.11.2016)

## VII.2. Členstvo v domácich spoločnostiach a organizáciách<sup>2</sup>

- **prof. RNDr. Igor Bock, PhD.** je členom JSMF, SSM
- **RNDr. Igor Brilla, PhD.** je členom SSM
- **prof. RNDr. Otokar Grošek, PhD.** je členom JSMF
- **RNDr. Mária Kečkemétyová, PhD.** je členkou JSMF
- **RNDr. Ivica Marinová, PhD.** je členkou JSMF
- **doc. RNDr. Ľubomír Marko, PhD.** je členom SSM
- **doc. RNDr. Karol Nemoga, PhD.** je členom JSMF a Slovenského plynárenského a naftového zväzu
- **doc. RNDr. Vladimír Olejček, PhD.** je členom JSMF
- **prof. Dr. Ing. Miloš Oravec** je členom SKSI
- **RNDr. Elena Pastuchová, PhD.** je členkou JSMF a Slovenskej štatistickej a demografickej spoločnosti
- **doc. Mgr. Marcel Polakovič, PhD.** je členom JSMF
- **doc. RNDr. Boris Rudolf, PhD.** je členom JSMF
- **doc. RNDr. Michal Zajac PhD.** je členom JSMF

## VII.3. Vedenie prác študentov v sút'aziach

---

<sup>2</sup> JSFM - Jednota slovenských matematikov a fyzikov

SSM - Slovenskej spoločnosti pre mechaniku

SSKI - Slovenská spoločnosť pre kybernetiku a informatiku

SBIMI - Spoločnosť biomedicínskeho inžinierstva a medicínskej informatiky

## VIII. PUBLIKÁCIE

### ACB Vysokoškolské učebnice vydané v domácich vydavateľstvách

ACB01 NÁNÁSIOVÁ, Oľga - KOHNOVÁ, Silvia. *Štatistika a pravdepodobnosť: Základy matematickej štatistiky a teórie pravdepodobnosti*. 1. vyd. Bratislava: Vydavateľstvo STU, 2016. 199 s. Edícia vysokoškolských učebníc. ISBN 978-80-227-4527-7.

### ADC Vedecké práce v zahraničných karentovaných časopisoch

ADC01 BOCK, Igor - JARUŠEK, Jiří - ŠILHAVÝ, Miroslav. On the solutions of a dynamic contact problem for a thermoelastic von Kármán plate. In *Nonlinear Analysis : Real World Applications*. Vol. 32, (2016), s. 111-135. ISSN 1468-1218. V databáze: SCOPUS: 2-s2.0-84966376452 ; CC: 000380079900008.

ADC02 OMELINA, Ľuboš - JANSEN, Bart - BONNECHÉRE, Bruno - ORAVEC, Miloš - PAVLOVIČOVÁ, Jarmila - VAN SINT, Jan Serge. Interaction Detection with Depth Sensing and Body Tracking Cameras in Physical Rehabilitation. In *Methods of Information in Medicine*. Vol. 55, Iss. 1 (2016), s. 70-78. ISSN 0026-1270. V databáze: CC: 000367827600010.

### ADE Vedecké práce v ostatných zahraničných časopisoch

ADE01 BOHDALOVÁ, Mária - KALINA, Martin - NÁNÁSIOVÁ, Oľga. Granger causality from a different viewpoint. In *Informační bulletin České statistické společnosti*. Roč. 27, č. 2 (2016), s. 23-28. ISSN 1210-8022.

ADE02 JUHÁSOVÁ, Ana - JUHÁS, Gabriel. Detection of livelocks and deadlocks in resource constrained workflow nets. In *Petri Net Newsletter*. Vol. 85, (2016), s. 25-44. ISSN 0391-1804.

ADE03 QI, Feng - ČERNANOVÁ, Viera. Some discussions on a kind of improper integrals. In *International Journal of Analysis and Applications*. Vol. 11, No. 2 (2016), s. 101-109. ISSN 2291-8639.

### ADM Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS

ADM01 HORÁK, Peter - HROMADA, Viliam. On a tiling paradox. In *Journal of Combinatorial Mathematics and Combinatorial Computing*. Vol. 96, (2016), s. 65-102. ISSN 0835-3026. V databáze: SCOPUS: 2-s2.0-84971441778.

### ADN Vedecké práce v domácich časopisoch registrovaných v databázach Web of Science alebo SCOPUS

ADN01 REPKA, Marek. Note on modular reduction in extended finite fields and polynomial rings for simple hardware. In *Journal of Electrical Engineering*. Vol. 67, No. 1 (2016), 56-60. ISSN 1335-3632. V databáze: SCOPUS: 2-s2.0-84962109402.

### AFC Publikované príspevky na zahraničných vedeckých konferenciách

AFC01 ANTAL, Eugen. Nature-inspired heuristic methods in classical cipher cryptanalysis. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 25-33. ISBN 978-80-227-4541-3.

- AFC02 BRILLA, Igor - JANIČEK, František. Numerical determination of voltage potential inside 2D anisotropic media using variational methods. In *Aplicaciones de las ciencias 2016 : Tercer congreso multidisciplinario de ciencias aplicadas en Latinoamérica (COMCAPLA 2016)*. La Habana, Cuba. 6-9 diciembre, 2016. Azcapotzalco : Universidad Autónoma Metropolitana, 2016, S. 360-366. ISBN 978-607-28-0912-3.
- AFC03 ČAVOJSKÝ, Maroš - DROZDA, Martin. Energy efficient trajectory recording of mobile devices using WiFi scanning. In *UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld 2016 [elektronický zdroj] : Conferences and workshops. Toulouse, France. July 18-21, 2016*. Piscataway : IEEE, 2016, USB, S. 1079-1085. ISBN 978-1-5090-2770-5. V databáze: IEEE ; SCOPUS: 2-s2.0-8501317401.
- AFC04 FABŠIČ, Tomáš - GALLO, Ondrej. Acoustic cryptanalysis. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 34-38. ISBN 978-80-227-4541-3.
- AFC05 HAMBALÍK, Alexander - MARÁK, Pavol. Possibilities of software recognition of small irregular patterns in biometrics for purposes of fingerprint analysis. In *XXIXth DIDMATTECH 2016: : New methods and technologies in education and practice, 1. part. International Scientific and Professional Conference, Budapest 25-26 August 2016*. 1. vyd. Budapešť : Tribun EU, 2016, S. 41-54. ISBN 978-963-284-799-3.
- AFC06 HAMBALÍK, Alexander - MARÁK, Pavol. Design and implementation of software support for biometrics laboratory courses. In *Trendy ve vzdělávání*. Roč. 9, č. 1 : Konference s mezinárodní účastí. Olomouc, Česká republika. 16-17.6.2016 (2016), online s. 75-83. ISSN 1805-8949.
- AFC07 JUHÁS, Gabriel - LORENZ, Robert. Synthesis of bounded petri nets from prime event structures with cutting context. In *ATEAED'2016 : Workshop on algorithms and theories for the analysis of event data. Torun, Poland. June 20-21, 2016*. Vol. 1592 ATEAED'2016, (2016), s. 58-77. ISSN 1613-0073. V databáze: SCOPUS: 2-s2.0-84977515573.
- AFC08 KAJAN, Michal - ORAVEC, Miloš - PAVLOVIČOVÁ, Jarmila - KURILOVÁ, Veronika. Determination of bright lesions in fundus images. In *Proceedings ELMAR-2016 : 58th International symposium. Zadar, Croatia. 12-14 September, 2016*. Zagreb : University of Zagreb, 2016, S. 77-80. ISSN 1334-2630. ISBN 978-953-184-221-1.
- AFC09 MARÁK, Pavol - HAMBALÍK, Alexander. A two-stage fingerprint feature extraction system for low quality fingerprint images. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 46-51. ISBN 978-80-227-4541-3.
- AFC10 MARČEK, Stanislav - DROZDA, Martin. Predicting system failures on mobile devices. In *Lecture Notes in Electrical Engineering*. Vol. 381 MedCT 2015, Vol. 2 : Mediterranean conference on information & communication technologies. Saidia, Morocco. May 7-9, 2015. Berlin : Springer, (2016), s. 499-508, ISBN 978-3-319-30296-6. ISSN 1876-1100.

- AFC11 OREM, Martin - ZAJAC, Pavol. Secure implementation of McEliece cryptosystem. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 52-56. ISBN 978-80-227-4541-3.
- AFC12 SOPIAK, Dominik - ORAVEC, Miloš - PAVLOVIČOVÁ, Jarmila - BUKOVČIKOVÁ, Zuzana - DITTINGEROVÁ, Monika - BILANSKÁ, Alexandra - NOVOTNÁ, Mária - GONTKOVIČ, Jozef. Generating face images based on 3D morphable model. In *ICNC-FSKD 2016 : 12th International conference on natural computation, fuzzy systems and knowledge discovery. Changsha, China. August 13-15, 2016*. Piscataway : IEEE, 2016, S. 58-62. ISBN 978-1-5090-4093-3. V databáze: IEEE ; SCOPUS: 2-s2.0-84997751445 ; WOS: 000386658300011.
- AFC13 VARGA, Juraj. Overview of android security mechanisms. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 59-64. ISBN 978-80-227-4541-3.
- AFC14 ZAJAC, Pavol. Some notes on MRHS equations over  $GF(2)$  with two left-hand sides. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 65-70. ISBN 978-80-227-4541-3.

#### **AFD Publikované príspevky na domácich vedeckých konferenciách**

- AFD01 BRILLA, Igor - JANIČEK, František. Numerical solution of boundary inverse problems of electrical conductivity for 3D anisotropic media. In *Power engineering 2016. Energy-Ecology-Economy 2016 : 13th International scientific conference. Tatranske Matliare, Slovakia. May 31 - June 2, 2016*. 1. vyd. Bratislava : Slovak University of Technology, 2016, S. 172-177. ISBN 978-80-89402-86-1.
- AFD02 JUHÁSOVÁ, Ana - KAZLOV, Igor - JUHÁS, Gabriel - MOLNÁR, Ľudovít. How to model curricula and learnflows by Petri nets - a survey. In *ICETA 2016 : 14th IEEE International conference on emerging elearning technologies and applications. Starý Smokovec, Slovakia. November 24 - 25, 2016*. Danvers : IEEE, 2016, S. 147-152. ISBN 978-1-5090-4701-7. V databáze: IEEE.
- AFD03 LESAY, Boris - PAVLOVIČOVÁ, Jarmila - ORAVEC, Miloš - KURILOVÁ, Veronika. Optic disc localization in fundus image. In *IWSSIP 2016 : 23th International conference on systems, signals and image processing. Bratislava, Slovakia. 23-25 May 2016*. 1. vyd. Bratislava : Slovak University of Technology in Bratislava, 2016, S. 125-128. ISBN 978-1-4673-9555-7. V databáze: IEEE ; SCOPUS: 2-s2.0-84978872988.
- AFD04 ORAVEC, Miloš - PAVLOVIČOVÁ, Jarmila - SOPIAK, Dominik - JIRKA, Vojtěch - LODERER, Marek - LEHOTA, Ľuboš - VODIČKA, Marek - FAČKOVEC, Matej - MIHALIK, Matej - TOMÍK, Martin - GERÁT, Jozef. Mobile ear recognition application. In *IWSSIP 2016 : 23th International conference on systems, signals and image processing. Bratislava, Slovakia. 23-25 May 2016*. 1. vyd. Bratislava : Slovak University of Technology in Bratislava, 2016, S. 121-124. ISBN 978-1-4673-9555-7. V databáze: IEEE ; SCOPUS: 2-s2.0-84978880145.



### **AFG Abstrakty príspevkov zo zahraničných konferencií**

- AFG01 FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam. Simple power analysis of McEliece cryptosystem on STM32F4 and Altera cyclone. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 57-58. ISBN 978-80-227-4541-3.
- AFG02 ŠRÁMKA, Michal. Practice-oriented computation of privacy risks in social networks from the user's perspective. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 1. ISBN 978-80-227-4541-3.

### **AFH Abstrakty príspevkov z domácich konferencií**

- AFH01 BOHDALOVÁ, Mária - KALINA, Martin - NÁNÁSIOVÁ, Oľga. QL-copulas, s-maps and conditioning on orthomodular lattices. In *FSTA 2016 : abstracts. Thirteenth International Conference on Fuzzy Set Theory and Applications. Liptovský Ján, SR, 24. - 29. 1. 2016*. 1. vyd. Liptovský Mikuláš : Armed Forces Academy of General M. R. Štefánik, 2016, S. 24. ISBN 978-80-8040-526-7.

### **BDM Odborné práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS**

- BDM01 MATYÁŠ, Václav - ŘÍHA, Zdeněk - ZAJAC, Pavol. Special issue on applied cryptography - Guest editorial. In *Infocommunications journal*. Vol. 8, Iss. 1 (2016), s. 1. ISSN 2061-2079. V databáze: WOS: 000382864400001.

### **BEE Odborné práce v zahraničných zborníkoch (konferenčných aj nekonferenčných)**

- BEE01 GULÁŠOVÁ, Michala. Steganalysis of StegoStorage. In *Mikulášská kryptobesídka 2016 : zborník príspevků. Praha, ČR, 1. - 2. 12. 2016*. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2016, S. 37-38. ISBN 978-80-904257-8-1.
- BEE02 SOVIČ, Tomáš - ANTAL, Eugen. Comparison of selected rotor ciphers. In *Mikulášská kryptobesídka 2016 : zborník príspevků. Praha, ČR, 1. - 2. 12. 2016*. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2016, S. 41-42. ISBN 978-80-904257-8-1.

### **BEF Odborné práce v domácich zborníkoch (konferenčných aj nekonferenčných)**

- BEF01 ANTAL, Eugen. Modern cryptanalysis of classical ciphers. In *CECC 2016 : The 16th central european conference on cryptology. Piestany, Slovakia. June 22 - 24, 2016*. Bratislava : STU, 2016, S. 29-33.
- BEF02 BOLEDOVIČ, Andrej - VARGA, Juraj. Practical implementation of McEliece cryptosystem on android. In *CECC 2016 : The 16th central european conference on cryptology. Piestany, Slovakia. June 22 - 24, 2016*. Bratislava : STU, 2016, S. 15-18.
- BEF03 GROŠEK, Otokar - HROMADA, Viliam. On generation of error vectors. In *CECC 2016 : The 16th central european conference on cryptology. Piestany, Slovakia. June 22 - 24, 2016*. Bratislava : STU, 2016, S. 97-100.

- BEF04 GULÁŠOVÁ, Michala - JÓKAY, Matúš. Steganalysis of stegostorage library. In *CECC 2016 : The 16th central european conference on cryptology. Piestany, Slovakia. June 22 - 24, 2016*. Bratislava : STU, 2016, S. 25-27.
- BEF05 HROMADA, Viliam - JÓKAY, Matúš - PROCHÁZKA, Matej - VOJVODA, Milan. Some weaknesses in one 3-quasigroup based encryption scheme. In *CECC 2016 : The 16th central european conference on cryptology. Piestany, Slovakia. June 22 - 24, 2016*. Bratislava : STU, 2016, S. 35-38.
- BEF06 ZAJAC, Pavol. On families of MRHS equations that can be solved in polynomial time. In *CECC 2016 : The 16th central european conference on cryptology. Piestany, Slovakia. June 22 - 24, 2016*. Bratislava : STU, 2016, S. 84-85.

#### **BFA Abstrakty odborných prác zo zahraničných podujatí (konferencie...)**

- BFA01 BOCK, Igor. Dynamic contact of a thermoelastic Mindlin-Timoshenko beam with a rigid obstacle. In *ETAMM 2016 : Book of Abstracts. Emerging trends in applied mathematics and mechanics. Perpignan, France. May 30 - June 3, 2016*. Perpignan : University of Perpignan Via Domitia, 2016, S. 35.

#### **DAI Dizertačné a habilitačné práce**

- DAI01 KOLLÁR, Jozef. *Štatistická analýza textov pre potreby kryptoanalýzy : dát. obhaj. 21.11.2016, č. ved. odboru 9-2-9*. Bratislava :STU v Bratislave FEI,2016. 144 s. Dostupné na internete: <[http://is.stuba.sk/zp/portal\\_zp.pl?podrobnosti=73053](http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=73053)>.
- DAI02 MARČEK, Stanislav. *Využitie kaskádovej klasifikácie pre detekciu chýb, systémových zlyhaní a sieťových prienikov*. 2016. Dostupné na internete: <[http://is.stuba.sk/zp/portal\\_zp.pl?podrobnosti=112041](http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=112041)>.
- DAI03 OMELINA, Ľuboš. *Vizuálne rozpoznávanie a identifikácia jednotlivca : dát. obhaj. 14.11.2016, č. ved. odboru 9-2-9*. Bratislava :STU v Bratislave FEI,2016. 167 s. Dostupné na internete: <[http://is.stuba.sk/zp/portal\\_zp.pl?podrobnosti=140735](http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=140735)>.

#### **FAI Redakčné a zostavovateľské práce knižného charakteru (bibliografie, encyklopédie, katalógy, slovníky, zborníky...)**

- FAI01 GROŠEK, Otokar (ed.) - HELLESETH, Tor (ed.) - KHOLOSHA, A. (ed.) - NEMOGA, Karol (ed.) - SEMAEV, Igor (ed.) - ZAJAC, Pavol (ed.). *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016. 79 s. ISBN 978-80-227-4541-3.

#### **Štatistika: kategória publikačnej činnosti**

ACB	Vysokoškolské učebnice vydané v domácich vydavateľstvách	1
ADC	Vedecké práce v zahraničných karentovaných časopisoch	2
ADE	Vedecké práce v ostatných zahraničných časopisoch	3
ADM	Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS	1
ADN	Vedecké práce v domácich časopisoch registrovaných v databázach Web of Science alebo SCOPUS	1
AFC	Publikované príspevky na zahraničných vedeckých konferenciách	14
AFD	Publikované príspevky na domácich vedeckých konferenciách	4

AFG	Abstrakty príspevkov zo zahraničných konferencií	2
AFH	Abstrakty príspevkov z domácich konferencií	1
BDM	Odborné práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS	1
BEE	Odborné práce v zahraničných zborníkoch (konferenčných aj nekonferenčných)	2
BEF	Odborné práce v domácich zborníkoch (konferenčných aj nekonferenčných)	6
BFA	Abstrakty odborných prác zo zahraničných podujatí (konferencie...)	1
DAI	Dizertačné a habilitačné práce	3
FAI	Redakčné a zostavovateľské práce knižného charakteru (bibliografie, encyklopédie, katalógy, slovníky, zborníky...)	1
<b>Súčet</b>		<b>43</b>

## IX. VÝCHOVA VEDECKÝCH PRACOVNÍKOV

### IX.1. Interní doktorandi

**Doktorand:** Ing. Eugen Antal

**Školiteľ:** prof. RNDr. Otokar Grošek, PhD.

**Školiteľ špecialista:** Mgr. Marek Sýs, PhD.

**Forma vzdelávania:** doktorandské štúdium – interná forma

**Odbor:** Aplikovaná informatika

**Pracovisko:** ÚIM, FEI STU

**Dizertačná skúška:** 5.6.2013

**Predpokladaný termín ukončenia:** marec 2017

**Téma práce:** Moderná kryptoanalýza klasických šifrier

**Doktorand:** Ing. Maroš Čavojský

**Školiteľ:** Dr.rer.nat. Martin Drozda

**Forma vzdelávania:** doktorandské štúdium – interná forma

**Odbor:** Aplikovaná informatika

**Pracovisko:** ÚIM, FEI STU

**Dizertačná skúška:** 18.2.2016

**Predpokladaný termín ukončenia:** 31.5.2017

**Téma práce:** Metodológia a systém na efektívne testovanie mobilných aplikácií

**Doktorand:** Mgr. Tomáš Fabšič

**Školiteľ:** prof. RNDr. Otokar Grošek, PhD.

**Forma vzdelávania:** doktorandské štúdium – interná forma

**Odbor:** Aplikovaná informatika

**Pracovisko:** ÚIM, FEI STU

**Dizertačná skúška:** 30.9.2015

**Predpokladaný termín ukončenia:** 31.8.2017

**Prerušenie:** 1.2.-2.9.2014

**Téma práce:** Postranné kanály

**Doktorand:** Ing. Michala Gulášová  
**Školiteľ:** doc. Ing. Milan Vojvoda, PhD.  
**Forma vzdelávania:** doktorandské štúdium – interná forma  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM, FEI STU  
**Dizertačná skúška:**  
**Predpokladaný termín ukončenia:** 31.8.2019  
**Téma práce:** Steganografia a stegoanalýza

**Doktorand:** Ing. Vojtěch Jirka  
**Školiteľ:** prof. Dr. Ing. Miloš Oravec  
**Forma vzdelávania:** doktorandské štúdium – interná forma  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM, FEI STU  
**Dizertačná skúška:** 22.5.2014  
**Predpokladaný termín ukončenia:** 31.8.2015  
**Prerušenie:** 1.7.2015-29.6.2017  
**Téma práce:** Nové metódy biometrického rozpoznávania tváří v neriadených podmienkach využitím metód strojového učenia

**Doktorand:** Ing. Pavol Marák  
**Školiteľ:** prof. RNDr. Otokar Grošek, PhD.  
**Školiteľ špecialista:** Ing. Alexander Hambalík, PhD.  
**Forma vzdelávania:** doktorandské štúdium – interná forma  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM, FEI STU  
**Dizertačná skúška:** 25.4.2015  
**Predpokladaný termín ukončenia:**  
**Téma práce:** Charakteristické vlastnosti odtlačkov prstov a dlaní a ich automatické rozpoznávanie

**Doktorand:** Ing. Ľuboš Omelina  
**Školiteľ:** prof. Dr. Ing. Miloš Oravec  
**Forma vzdelávania:** doktorandské štúdium – interná forma  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM, FEI STU  
**Dizertačná skúška:** 28.2.2011  
**Prerušenie:** 1.11.2011-31.1.2013 a 15.11.2015-15.11.2016  
**Téma práce :** Návrh metód rozpoznávania vzorov v biometrii  
**Ukončenie:** 14.11.2016

**Doktorand:** Ing. Alexandra Posoldová  
**Školiteľ:** prof. Dr. Ing. Miloš Oravec  
**Forma vzdelávania:** doktorandské štúdium – interná forma  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM, FEI STU  
**Dizertačná skúška:** 11.6.2014  
**Predpokladaný termín ukončenia:** 31.8.2015  
**Prerušenie:** 26.6.2014-28.6.2016

**Téma práce:** Metodológia a algoritmy predikcie správania používateľa pre personalizáciu prostredia v HBBTv  
**Vyradenie:** 29.7.2016

**Doktorand:** Ing. Dominik Sopiak  
**Školiteľ:** prof. Dr. Ing. Miloš Oravec  
**Forma vzdelávania:** doktorandské štúdium – interná forma  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM, FEI STU  
**Dizertačná skúška:** 16.5.2016  
**Predpokladaný termín ukončenia:** 31.5.2017  
**Téma práce:** Návrh multimodálneho biometrického systému

**Doktorand:** Ing. Juraj Varga  
**Školiteľ:** doc. Ing. Pavol Zajac, PhD.  
**Forma vzdelávania:** doktorandské štúdium – interná forma  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM, FEI STU  
**Dizertačná skúška:** 14.6.2013  
**Predpokladaný termín ukončenia:**  
**Téma práce:** Bezpečnosť mobilných zariadení

## **IX.2. Externí doktorandi**

**Doktorand:** Ing. Robert Bučko  
**Školiteľ:** doc. RNDr. Jaroslav Fogel, PhD.  
**Forma vzdelávania:** doktorandské štúdium – externá forma  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM FEI STU  
**Dizertačná skúška:** 09.2012  
**Predpokladaný termín ukončenia:** 31.8.2015  
**Téma práce:** Verifikačné metódy v multiagentových systémoch

**Doktorand:** Ing. Csaba Cserba  
**Školiteľ:** prof. RNDr. Gabriel Juhás, PhD.  
**Forma vzdelávania:** doktorandské štúdium – externá forma  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM, FEI STU  
**Dizertačná skúška:**  
**Predpokladaný termín ukončenia:**  
**Téma práce:**

**Doktorand:** Ing. Igor Kazlov  
**Školiteľ:** prof. RNDr. Gabriel Juhás, PhD.  
**Forma vzdelávania:** doktorandské štúdium – externá forma od 1.6.2014, interná forma do 31.5.2014  
**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM, FEI STU

**Dizertačná skúška:** 14.11.2012

**Predpokladaný termín ukončenia:** 30.8.2013

**Téma práce:** Analýza udalostných systémov s viacerými inštanciami

**Doktorand:** Mgr. Jozef Kollár

**Školiteľ:** prof. RNDr. Otokar Grošek, PhD.

**Forma vzdelávania:** doktorandské štúdium – interná 1.9.2010 externá forma od novembra 2012

**Odbor:** Aplikovaná informatika

**Pracovisko:** ÚIM, FEI STU

**Dizertačná skúška:** 28.2.2012

**Predpokladaný termín ukončenia:** 30.8.2015

**Prerušenie:** 1.9.2014-30.8.2016

**Téma práce:** Štatistická analýza textov pre potreby kryptoanalýzy

**Ukončené:** 21.11.2016

**Doktorand:** MUDr. Veronika Kurilová (rod. Hanúsková)

**Školiteľ:** prof. Dr. Ing. Miloš Oravec

**Forma vzdelávania:** doktorandské štúdium – externá forma

**Odbor:** Aplikovaná informatika

**Pracovisko:** ÚIM FEI STU

**Dizertačná skúška:** 29.4.2014

**Predpokladaný termín ukončenia:**

**Téma práce:** Nové metódy diagnostiky v oftalmológii

**Prerušenie:** 1.9.2016-2.9.2018

**Doktorand:** Ing. Stanislav Marček

**Školiteľ:** prof. RNDr. Gabriel Juhás, PhD.

**Forma vzdelávania:** doktorandské štúdium – externá forma od 1.9.2013, interná od 1.10.2007 do 1.9.2013

**Odbor:** Aplikovaná informatika

**Pracovisko:** ÚIM, FEI STU

**Dizertačná skúška:** 17.6.2010

**Téma práce:** Modelovanie a simulácia udalostných systémov

**Ukončené:** 31.8.2016

**Doktorand:** Ing. Peter Minarovský

**Školiteľ:** doc. Ing. Michal Šrámka, PhD.

**Forma vzdelávania:** doktorandské štúdium – externá forma

**Odbor:** Aplikovaná informatika

**Pracovisko:** ÚIM, FEI STU

**Dizertačná skúška:**

**Predpokladaný termín ukončenia:** máj 2020

**Téma práce:** Unikátnosť kódu

**Doktorand:** Mgr. Zuzana Ševčíková

**Školiteľ:** prof. RNDr. Gabriel Juhás, PhD.

**Forma vzdelávania:** doktorandské štúdium – externá forma

**Odbor:** Aplikovaná informatika  
**Pracovisko:** ÚIM FEI STU  
**Dizertačná skúška:** 28.8.2013  
**Predpokladaný termín ukončenia:** 30.9.2014  
**Prerušenie:** 28.8.2013-1.9.2015  
**Téma práce:** Nesekvenčná sémantika Petriho sietí  
**Vyradenie:** 1.9.2016

**Doktorand:** Mgr. Tomáš Žilka  
**Školiteľ:** prof. RNDr. Igor Bock, PhD.  
**Prijatý dňa:** 8.7.2010  
**Forma vzdelávania:** doktorandské štúdium – externá forma od 2.9.2015  
**Odbor:** 9.1.9 Aplikovaná matematika  
**Pracovisko:** OM ÚIM FEI STU v Bratislave  
**Dátum dizertačnej skúšky:** 28.2.2012  
**Predpokladaný termín ukončenia:** 31.8.2016  
**Prerušenie:** 1.9.2014-1.9.2015  
**Téma práce:** Dynamický kontakt dosky s prekážkou

**Doktorand:** Mgr. Viktória Žilková (rod. Rozborová)  
**Školiteľ:** doc. RNDr. Michal Zajac, PhD.  
**Prijatá dňa:** 8.7.2010  
**Forma vzdelávania:** doktorandské štúdium – externá forma od 2.9.2015  
**Odbor:** 9.1.9 Aplikovaná matematika  
**Pracovisko:** OM ÚIM FEI STU v Bratislave  
**Dátum dizertačnej skúšky:** 28.2.2012  
**Predpokladaný termín ukončenia:** 31.8.2016  
**Prerušenie:** 1.9.2014-1.9.2015  
**Téma práce:** Hyperreflexívnosť priestorov lineárnych operátorov

### **IX.3. Doktorandi vedení pracovníkmi ÚIM na iných pracoviskách**

**Doktorand:** Ing. Dušan Janál  
**Školiteľ:** doc. RNDr. Oľga Nánásiová, PhD.  
**Forma vzdelávania:** doktorandské štúdium – denná forma  
**Odbor:** 9.1.9 Aplikovaná matematika  
**Pracovisko:** Katedra matematiky a deskriptívnej geometrie  
**Predpokladaný termín ukončenia:** 5.9.2017  
**Téma práce:** Viacrozmerné štatistické metódy a ich aplikácie

## **X. ÚČASŤ PRACOVNÍKOV ÚSTAVU NA KONFERENCIÁCH**

### **X.1. Zahraničné konferencie**

**NÁZOV KONFERENCIE :** Norwegian-Slovakian Workshop in Crypto  
**Miesto:** Bergen, Nórsko  
**Dátum:** 6. - 11. 2. 2016  
**Meno:** Ing. Viliam Hromada, PhD.

**Príspevok:** Simple Power Analysis of McEliece Cryptosystem on STM32 and Altera Cyclone

**NÁZOV KONFERENCIE :** Cryptoaction symposium 2016

**Miesto:** Budapešť, Maďarsko

**Dátum:** 6.-8.4.2016

**Meno:** doc. Ing. Pavol Zajac, PhD.

**NÁZOV KONFERENCIE :** Historical Ciphers Colloquium HCC 2016

**Miesto:** Kassel, Nemecko

**Dátum:** 4.-6.5.2016

**Meno:** Ing. Eugen Antal

**NÁZOV KONFERENCIE :** Workshop z numerickej matematiky

**Miesto:** Ostrava, Česká republika

**Dátum:** 5.-6.5.2016

**Meno:** prof. RNDr. Igor Bock, PhD.

**Príspevok:** An optimal design problem for a viscoelastic plate in a dynamic contact

**NÁZOV KONFERENCIE :** Emerging Trends in Applied Mathematics and Mechanics ETAMM 2016

**Miesto:** Perpignan, Francúzsko

**Dátum:** 30.5.-3.6.2016

**Meno:** prof. RNDr. Igor Bock, PhD.

**Príspevok:** Dynamic contact of a thermo-elastic Mindlin-Timoshenko beam with a rigid obstacle

**NÁZOV KONFERENCIE :** Trendy ve vzdělávání 2016

**Miesto:** Olomouc, Česká republika

**Dátum:** 15.-17.6.2016

**Meno:** Ing. Alexander Hambalík, PhD.

**Príspevok:** Design and implementations of software support for biometrics laboratory courses

**NÁZOV KONFERENCIE :** Algorithms and Theories for Analysis of Event Data *ATAED 2016*

**Miesto:** Torun, Poľsko

**Dátum:** 19.-22.6.2016

**Meno:** prof. RNDr. Gabriel Juhás, PhD.

**Príspevok:** Synthesis of bounded Petri Nets from Prime Event Structures with Cutting Cintext

**NÁZOV KONFERENCIE :** International Quantum Structures Association *IQSA 2016*

**Miesto:** Leicester, V. Británia

**Dátum:** 11.-16.7.2016

**Meno:** doc. RNDr. Oľga Nánásiová, PhD.

**Príspevok:** BELL'S INEQUALITIES VIA S-MAP



**NÁZOV KONFERENCIE :** Artic Crypt 2016

**Miesto:** Longyearbyen, Svalbard, Nórsko

**Dátum:** 17.-22.7.2016

**Meno:** Mgr. Tomáš Fabšič, prof. RNDr. Otokar Grošek, PhD., doc. RNDr. Karol

**Nemoga, PhD., doc. Ing. Pavol Zajac, PhD.**

**Príspevok:** On generating invertible circulant binary matrices with a prescribed number of ones

**NÁZOV KONFERENCIE :** International Conference on UIC 2016

**Miesto:** Toulouse, Francúzsko

**Dátum:** 16.-23.7.2016

**Meno:** Ing. Maroš Čavojský

**Príspevok:** Energy Efficient Trajectory Recording of Mobile Devices Using WiFi Scanning

**NÁZOV KONFERENCIE :** 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery

**Miesto:** Changsha, China

**Dátum:** 13.-15.8.2016

**Meno:** Ing. Dominik Sopiak

**Príspevok:** General face images based on 3D Morphable Model

**NÁZOV KONFERENCIE :** XXIXth DIDMATTECH 2016

**Miesto:** Budapešť

**Dátum:** 25.-26.8.2016

**Meno:** Ing. Alexander Hambalík, PhD.

**Príspevok:** Possibilities of software recognition of small irregular patterns in biometrics for purposes of fingerprint analysis

**NÁZOV KONFERENCIE :** Workshop on Secure Implementation of Post-Quantum Cryptography

**Miesto:** Tel-Aviv, Izrael

**Dátum:** 24. - 29. 9. 2016

**Meno:** Ing. Viliam Hromada, PhD.

**Príspevok:** Side-channel Analysis of McEliece Cryptosystem

**NÁZOV KONFERENCIE :** III Congreso Multidisciplinario de Ciencias Aplicadas en Latinoamerica *COMCAPLA 2016*

**Miesto:** Havana, Kuba

**Dátum:** 5.-11.12.2016

**Meno:** RNDr. Igor Brilla, PhD.

**Príspevok:** Numerical Determination of Voltage Potential Inside 2D Anisotropic Media Using Variational Methods

**NÁZOV KONFERENCIE :** Mikulášska kryptobesídka 2016

**Miesto:** Praha, Česká republika

**Dátum:** 1.-2.12.2016

**Meno:** Ing. Michala Gulášová

**Príspevok:** Steganalysis of Stegostorage

**NÁZOV KONFERENCIE :** Mikulášska kryptobesídka 2016

**Miesto:** Praha, Česká republika  
**Dátum:** 1.-2.12.2016  
**Meno:** Ing. Eugen Antal

## **X.2. Domáce konferencie**

**NÁZOV KONFERENCIE :** The 23rd International Conference on Systems, Signals and Image Processing IWSSIP 2016

**Miesto:** Bratislava

**Dátum:** 23.-25.5.2016

**Meno:** Ing. Dominik Sopiak

**Príspevok:** Mobile Ear Recognition Application

**NÁZOV KONFERENCIE :** Energetika-Ekológia-Ekonomika EEE 2016

**Miesto:** Tatranské Matliare

**Dátum:** 31.5.-2.6.2016

**Meno:** RNDr. Igor Brilla, PhD.

**Príspevok:** Numerical solution of boundary inverse problems of electrical conductivity for 3D anisotropic media

**NÁZOV KONFERENCIE :** The 16th Central European Conference on Cryptology

**Miesto:** Piešťany

**Dátum:** 22.-24.6.2016

**Meno:** prof. RNDr. Otokar Grošek, PhD.

**Príspevok:** On Generation of Error Vectors

**NÁZOV KONFERENCIE :** The 16th Central European Conference on Cryptology

**Miesto:** Piešťany

**Dátum:** 22.-24.6.2016

**Meno:** Ing. Michala Gulášová

**Príspevok:** Steganalysis of Stegostorage Library

**NÁZOV KONFERENCIE :** The 16th Central European Conference on Cryptology

**Miesto:** Piešťany

**Dátum:** 22.-24.6.2016

**Meno:** Ing. Eugen Antal

**Príspevok:** Modern cryptanalysis of classical ciphers

**NÁZOV KONFERENCIE :** The 16th Central European Conference on Cryptology

**Miesto:** Piešťany

**Dátum:** 22.-24.6.2016

**Meno:** Ing. Viliam Hromada, PhD.

**Príspevok:** On Generation of Error Vectors

**NÁZOV KONFERENCIE :** The 16th Central European Conference on Cryptology

**Miesto:** Piešťany

**Dátum:** 22.-24.6.2016

**Meno:** doc. Ing. Pavol Zajac, PhD.

**Príspevok:** On families of MRHS equations that can be solved in polynomial time

## **XI. HABILITAČNÉ A INAUGURAČNÉ KONANIA**

### **XI.1. Inauguračné konania**

### **XI.2. Habilitačné konania**

### **XI.3. Členstvá v komisiách**

## **XII. ČINNOSŤ V OBLASTI DOKTORSKÝCH DIZERTAČNÝCH PRÁC (DrSc.) A DOKTORANDSKÝCH DIZERTAČNÝCH PRÁC**

### **XII.1. Obhajoby dizertačnej práce na ÚIM**

### **XII.2. Dizertačné skúšky na ÚIM**

**prof. RNDr. Otokar Grošek, PhD.** – predseda diz. Skúšky Dominika Sopiaka, 16.5.2016

### **XII.3. Dizertačné skúšky a obhajoby dizertačných prác na iných pracoviskách**

**prof. RNDr. Otokar Grošek, PhD.** – predseda obhaj. komisie Ing. Luboša Omelinu  
v Bruseli, 14.11.2016

**prof. RNDr. Igor Bock, PhD.** - člen komisie pre dizertačnú skúšku Mgr. Jána Komadela,  
FMFI UK, 10.06.2016

**prof. RNDr. Igor Bock, PhD.** - člen komisie pre dizertačnú skúšku Ing. Viery Kleinovej,  
Stav. Fak. STU 10.06.2016

**doc. RNDr. Michal Zajac, PhD.** - člen komisie na obhajobe dizertačnej práce Mgr. Kataríny  
Hriňákovej, KMDG SvF STU 30.8.2016

**doc. RNDr. Michal Zajac, PhD.** - člen komisie na obhajobe dizertačnej práce Mgr. Veroniky  
Hucíkovej, KMDG SvF STU 9.12.2016

### **XII.4. Oponentské posudky k dizertačnej práci**

**prof. RNDr. Igor Bock, PhD.** – oponent dizertačnej práce Ing. Petry Rozehnalovej, Fak. Strojního inženýrstva VUT Brno, obhájená dňa 04.03.2016

**prof. RNDr. Igor Bock, PhD.** – oponent dizertačnej práce Ing. Jozefa Urbána, Stav. Fak. STU, obhájená dňa 25.08.2016

**doc. RNDr. Michal Zajac, PhD.** - oponent dizertačnej práce Mgr. Márie Holecyovej, FMFI UK, obhájená dňa 24.8.2016

**doc. RNDr. Michal Zajac, PhD.** - oponent dizertačnej práce RNDr. Ivany Ilčíkovej, FMFI UK, obhájená dňa 30.8.2016

## **XII.5. Oponentské posudky k písomnej práci k dizertačnej skúške**

**prof. RNDr. Igor Bock, PhD.** – oponent písomnej práce Ing. Michala Kollára, Stav. Fak. STU, skúška 10.06.2016

## **XII.6. Skúšky z matematických predmetov doktorandského štúdia**

<b>Meno doktoranda</b>	<b>Odbor štúdia</b>	<b>Meno skúšajúceho</b>	<b>Predmet</b>	<b>Dátum</b>
Norbert Kaplan	Elektrotechnika	Prof. Bock	Aplikovaná matematika	10.02.2016
Robert Szobolovský	Mikroelektronika	Prof. Bock	Aplikovaná matematika	18.02.2016
Tomáš Bagala	Elektronika a fotonika	Prof. Bock	Aplikovaná matematika	29.06.2016
Adam Fibich	Elektronika a fotonika	Prof. Bock	Aplikovaná matematika	29.06.2016

## **XIII. ŠVOČ, VEDENIE DIPLOMOVÝCH PRÁC, ČLENSTVO V ŠTÁTNICOVÝCH KOMISIÁCH**

### **XIII.1. ŠVOČ**

#### **Sekcia: Aplikovaná informatika**

Komisia: doc. RNDr. Ľubomír Marko, PhD., - predseda  
Ing. Alexander Hambalík, PhD.  
Ing. Štefan Balogh, PhD.  
Ing. Viliam Hromada, PhD.  
Ing. Vladislav Novák – tajomník

Študent: **Radovan Bezák**:  $\mu$ Eliece: QC-MDPC Mc Eliece kryptosystém na mikropočesore (Cena dekana)

Vedúci: doc. Ing. Pavol Zajac, PhD.

Študent: **Tomáš Sovič**: Porovnanie vybratých rotorových šifrátorov (Cena sponzora HUMUSOFT)

Vedúci: Ing. Eugen Antal

Študent: **Tomáš Hlibový**: Lúštenie nezlomených klasických šifier (Cena sponzora LEGRAND)

Vedúci: Ing. Eugen Antal

Študent: **Jozef Úroda**: Neurónové siete a ich nasadenie v kritických fázach práce automatizovaného daktyloskopického systému (Cena ČS sekcie IEEE)

Vedúci: Ing. Pavol Marák

Študent: **Roderik Ploszek**: Testovacie prostredie pre systém Medusa (Diplom dekana)

Vedúci: Mgr. Ing. Matúš Jókay, PhD.

**Sekcia** : Matematicko-počítačové modelovanie, Stavebná fakulta STU

**Meno**: prof. RNDr. **Igor Bock, PhD.**

**Člen komisie** pre posúdenie prác Študentskej vedeckej konferencie

## XIII.2. VEDENIE UKONČENÝCH DIPLOMOVÝCH PRÁC

**Bachúriková Mária**: Počítačová podpora hodnotenia kvality zvarov prostredníctvom single-board počítačov (D. Rosinová, konz. E. Kučera)

**Bako Pavol**: Podpora identifikácie pohybu entít s využitím Beacon technológie (B. Mišota)

**Bednárík Jakub**: Konferenčné schémy pre mobilnú komunikáciu (K. Nemoga)

**Beke Roland**: Využitie mobilných aplikácií pre potreby manažmentu diabetických pacientov (F. Lehocki)

**Bölcš Štefan**: Open Data a využitie Graph databáz (F. Lehocki)

**Boledovič Andrej**: Využitie McElieceovho kryptosystému v prostredí OS Android (P. Zajac, konz. J. Varga)

**Briš Ladislav**: Využitie formalizmov Petriho sietí v riadení laboratórnych systémov (A. Kozáková, konz. E. Kučera)

**Czakó Gergely**: Sieťový systém v otvorenom kóde na efektívne rozpoznávanie markantov v daktyloskopických stopách - pre metódu "neurónové siete" (A. Hambalík)

**Češek Pavol**: Riadenie DEDES pomocou mikrokontrolérov s využitím Petriho sietí (A. Kozáková, konz. E. Kučera)

**Češková Alžbeta**: Riadenie laboratórnych udalostných systémov (D. Rosinová, konz. E. Kučera)

**Dano Andrej**: Online riadenie laboratórneho experimentu TOS1A (K. Žáková)

**Dobročka Pavol**: Podpisové schémy v postkvantovej kryptografii (P. Zajac)

**Fornádel Jakub**: Metóda potlačenia kmitov rezacieho stola (P. Hubinský, konz. M. Flassik)

**Freňak Mikuláš**: Cvakátka (M. Jókay)

**Gallovič Michal**: Manažovanie prístupu k online experimentom (K. Žáková)

**Gáži Tomáš**: Nepresnosti v spracovávaní obrazových predlôh odtlačkov prstov a ich možná eliminácia v praxi (A. Hambalík)

**Glonek Martin**: Biometria očnej dúhovky v mobilnom zariadení (M. Oravec, konz. V. Jirka)

**Goboňa Patrik**: Webová aplikácia pre analýzu dolovania dát (S. Marček)

**Gulášová Michala**: Stegoanalýza knižnice StegoStorage (M. Jókay)

**Gyurian Norbert**: Integrácia multimodálneho rozhrania v inteligentnej domácnosti (G. Rozinaj)

**Hanzlová Katarína:** Kvázigrupový šifrovací systém (M. Vojvoda)

**Hesko Ján:** Porovnanie databázových technológií Apache Hive a IBM BigSQL bežiacich na Big data platforme Apache Hadoop (F. Lehocki)

**Holba Pavol:** Analýza medicínskych dát pacientov s použitím "big data" technológií (F. Lehocki)

**Hoppán Matúš:** Návrh konceptu bezpečného produkčného klienta vo VW SK produkčnom prostredí (M. Drozda)

**Ižold Andrej:** Podpisové schémy (K. Nemoga)

**Jurčo-Glina Martin:** Webová aplikácia na sprístupnenie DNA analýz pre laboratórnych technikov (F. Lehocki)

**Kajan Michal:** Klasifikácia pre diagnostiku v oftalmológii (M. Oravec)

**Kollman Ľudovít:** Sieťový systém v otvorenom kóde na efektívne predspracovanie markantov v daktyloskopických stopách (A. Hambalík)

**Krajčír Martin:** Homomorfný kryptosystém (M. Sýs)

**Kraslan Mário:** Riadenie procesov na báze Petriho sietí (Z. Ševčíková)

**Kriško Miloslav:** Chybová analýza MPKC (V. Hromada)

**Kúdela Adam:** Identifikácia patogénnych organizmov z útržkov DNA (F. Lehocki)

**Kuffa Michal:** Detekcia anomálií v sieťach pomocou Netflow ako súčasť aktívnej sieťovej ochrany (K. Nemoga)

**Kupkovičová Alexandra:** Prúdové šifry z hľadiska praktickej implementácie (K. Nemoga)

**Kysel' Matúš:** Ďalší rozvoj knižnice StegoStorage (M. Jókay)

**Ledecký Boris:** Nástroje a procesy vo vývoji veľkých databázových aplikácií (I. Kossaczký)

**Macko Martin:** Bezpečnosť mobilných platieb (M. Šrámka)

**Máčaj Mário:** Komunitná platforma na podporu aktívneho životného štýlu (F. Lehocki)

**Mačák Matúš:** Aproximácia wattového výkonu športovca (S. Marček)

**Majzel Michal:** Android aplikácia pre snímanie a spracovanie odtlačkov prstov pomocou externého snímača (A. Hambalík)

**Markech Martin:** Využitie technológie hadoop na ukladanie sématických dát (I. Kossaczký)

**Matiaško Patrik:** Bezpečnostné senzory pre spracovanie veľkých dát s využitím ontológie (Š. Balogh)

**Mičuda Martin:** Prúdová šifra SPROUT (V. Hromada)

**Mokráš Róbert:** Spracovanie a analýza odtlačkov prstov pomocou viacjadrového procesora (A. Hambalík)

**Nemec Pavol:** Automatizovaný systém na spracovanie údajov zo SMART senzorov (M. Vojs)

**Novotný Daniel:** Overenie integrity OS Android (M. Šrámka)

**Orem Martin:** Bezpečná implementácia McEliece kryptosystému (P. Zajac)

**Packo Igor:** Moderná webová aplikácia pre správu skladov dreva (P. Bisták)

**Pavčiak Emil:** Akustický útok na RSA šifru (O. Gallo)

**Pethó Tibor:** Desynchronizačný útok na prúdové šifry (V. Hromada)

**Pintér Róbert:** Pokračovanie v riešení pre autentifikáciu softvérovým mobilným tokenom (M. Repka)

**Pištej Jozef:** Tvorba API pre online prístup k simulačnému prostrediu SciLab (K. Žáková)

**Pivarči Matej:** Strojové spracovanie a hodnotenie praktických úloh základov programovania (O. Grošek)

**Pivarník Ján:** Podpisové schémy na báze hašovacích funkcií (P. Zajac)

**Polačík Ivan:** Realizácia virtuálneho laboratória pomocou technológie PHP (P. Bisták)

**Potapov Oleksii:** Detection of Heart Failure Using Ontologies (F. Lehocki)

**Priščák Martin:** Vývoj a porovnanie blokových šifrier (K. Nemoga)

**Procházka Matej:** Cube Attack v kryptoanalýze prúdových šifrier (V. Hromada)

**Rábek Matej:** Správa komunikačných kanálov a služieb pre online laboratórium (K. Žáková)

**Račko Richard:** Analýza vlastností a správania softvérových systémov (Š. Balogh)

**Raddawi Khaled Jamal:** Strengthened Iterated Hill Cipher for Encrypted Processing (O. Grošek)

**Rajnic Dávid:** Rozšírená realita pre Android zariadenie (M. Drozda)

**Reingraber Radovan:** Možnosti synchronizácie kontextového obsahu vzhľadom na polohu na báze Beacon technológie (B. Mišota)

**Rehák Jakub:** Riadenie procesov na báze Petriho sietí (Z. Ševčíková)

**Simon Ádám:** Využitie moderných mobilných zariadení v automobilovom priemysle (S. Marček)

**Simonides Šimon:** Riešenie systému MRHS rovníc (P. Zajac)

**Smolko Ján:** Detekcia a určovanie 2D pozície tváre na minipočítači Raspberry Pi (M. Kukučka)

**Smreček František:** HMI animácia robustného riadenia (J. Kardoš)

**Stark Erich:** Tvorba virtuálneho laboratória s využitím JavaScript-u na strane servera (P. Bisták)

**Suchanovský Ján:** Vysoká dostupnosť webových služieb (O. Gallo)

**Svítek Matúš:** E-learning systém pre testovanie a hodnotenie praktických úloh z programovania (O. Grošek)

**Szabo Andrej:** White-Box kryptografia (M. Sýs)

**Turčina Pavol:** Rozpoznávanie a spracovanie znakov netextového charakteru (E. Antal)

**Turza Štefan:** Lightweight kryptosystémy s verejným kľúčom (V. Hromada)

**Šarmír Peter:** Útok na šifru Mc Eliece pomocou analýzy spotreby (O. Gallo)

**Vali Miroslav:** Priemyselné predspracovanie obrazu tváre na mobilnom zariadení v reálnom čase (M. Oravec)

**Varl Oliver:** Vodič, hudba a riadenie automobilu (M. Kukučka)

**Zima Milan:** Zber a evaluácia databázy očných dúhoviek (M. Oravec, konz. V. Jirka)

**Zimová Marcela:** Odtlačková funkcia BLAKE (K. Nemoga)

### XIII.3. ČLENSTVO V ŠTÁTNICOVÝCH KOMISIÁCH

- **Ing. Eugen Antal** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Ing. Eugen Antal** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Eugen Antal** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Ing. Štefan Balogh, PhD.**- člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Ing. Štefan Balogh, PhD.**- člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Štefan Balogh, PhD.**- člen štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Ing. Štefan Balogh, PhD.**- člen štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS

- **prof. RNDr. Igor Bock, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Ing. Maroš Čavojský** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Maroš Čavojský** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **RNDr. Viera Čerňanová, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **RNDr. Karla Čipková, PhD.** - člen štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Dr.rer.nat. Martin Drozda** - predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Dr.rer.nat. Martin Drozda** - predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Mgr. Tomáš Fabšič** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Mgr. Tomáš Fabšič** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Ing. Ondrej Gallo, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Ing. Ondrej Gallo, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Ondrej Gallo, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Ing. Ondrej Gallo, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **prof. RNDr. Otokar Grošek, PhD.** – predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **prof. RNDr. Otokar Grošek, PhD.** – predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **prof. RNDr. Otokar Grošek, PhD.** – predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **prof. RNDr. Otokar Grošek, PhD.** – predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Ing. Alexander Hambalík, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Ing. Alexander Hambalík, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Alexander Hambalík, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Ing. Alexander Hambalík, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Ing. Viliam Hromada, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Ing. Viliam Hromada, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Viliam Hromada, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS



- **Ing. Viliam Hromada, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Mgr. Ing. Matúš Jókay, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Mgr. Ing. Matúš Jókay, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Mgr. Ing. Matúš Jókay, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Mgr. Ing. Matúš Jókay, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **prof. RNDr. Gabriel Juhás, PhD.**- predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **prof. RNDr. Gabriel Juhás, PhD.**- predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **RNDr. Mária Kečkemétyová, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **RNDr. Igor Kossaczký, CSc.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **RNDr. Igor Kossaczký, CSc.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **RNDr. Igor Kossaczký, CSc.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Ing. Pavol Marák** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Ing. Pavol Marák** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Pavol Marák** - tajomník štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Ing. Stanislav Marček** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Stanislav Marček** - tajomník štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.7.2016 – doména MSUS
- **RNDr. Ivica Marinová, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **doc. RNDr. Ľubomír Marko, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **doc. RNDr. Ľubomír Marko, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **doc. RNDr. Ľubomír Marko, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **doc. RNDr. Ľubomír Marko, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **doc. RNDr. Oľga Nánásiová, PhD.** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **doc. RNDr. Oľga Nánásiová, PhD.** - člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **doc. RNDr. Oľga Nánásiová, PhD.** - člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS

- **doc. RNDr. Karol Nemoga, PhD.**- predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **doc. RNDr. Karol Nemoga, PhD.**- predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Ing. Vladislav Novák** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Ing. Vladislav Novák** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Vladislav Novák** - tajomník štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **doc. RNDr. Vladimír Olejček, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **doc. RNDr. Vladimír Olejček, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Mgr. Dávid Pancza, PhD.** - člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **RNDr. Elena Pastuchová, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **RNDr. Elena Pastuchová, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **doc. Mgr. Marcel Polakovič, PhD.** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **doc. Mgr. Marcel Polakovič, PhD.** - člen štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **doc. Mgr. Marcel Polakovič, PhD.** - člen štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **doc. RNDr. Boris Rudolf, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **doc. RNDr. Boris Rudolf, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **doc. RNDr. Boris Rudolf, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Ing. Dominik Sopiak** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Ing. Dominik Sopiak** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Mgr. Marek Sýs, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Mgr. Zuzana Ševčíková** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Mgr. Zuzana Ševčíková** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **doc. Ing. Michal Šrámka, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **Ing. Juraj Varga** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **Ing. Juraj Varga** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS

- **Ing. Juraj Varga** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **doc. Ing. Milan Vojvoda, PhD.** – predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **doc. Ing. Milan Vojvoda, PhD.** – predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **doc. Ing. Milan Vojvoda, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **doc. Ing. Milan Vojvoda, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **doc. RNDr. Michal Zajac, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **doc. RNDr. Michal Zajac, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **doc. RNDr. Michal Zajac, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **doc. RNDr. Michal Zajac, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **doc. Ing. Pavol Zajac, PhD.**- predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2016 – doména BIS
- **doc. Ing. Pavol Zajac, PhD.**- predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **doc. Ing. Pavol Zajac, PhD.**- predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 14.6.2016 – doména BIS
- **doc. Ing. Pavol Zajac, PhD.**- predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS
- **Mgr. Michal Zákopčan, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2016 – doména MSUS
- **Mgr. Michal Zákopčan, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 15.6.2016 – doména MSUS

## XIV. EDIČNÉ AKTIVITY

### XIV.1. Vydávanie časopisov

Oddelenie matematiky FEI STU v Bratislave je spolueditorom periodika Tatra Mountains Mathematical Publications. Hlavným editorom je MÚ SAV v Bratislave.

#### XVI.1.1 Editované čísla v roku 2016

**Special issue on applied cryptography** - Guest editorial, volume 8, issue 1 – **P. Zajac**

### XIV.2. Členstvá v redakčných radách časopisov

- **prof. RNDr. Otokar Grošek, PhD.** je členom redakčnej rady Tatra Mountains Mathematical Publications. (vydavateľstvo Walter de Gruyter).

- **prof. RNDr. Otokar Grošek, PhD.** je členom redakčnej rady Journal of Mathematical Cryptology (vydavateľstvo Walter de Gruyter)
- **prof. RNDr. Gabriel Juhás, PhD.** je členom redakčnej rady Transactions on Petri Nets and Other Models of Concurrency (vydavateľstvo Springer-Verlag)
- **doc. RNDr. Karol Nemoga, PhD.** je výkonný redaktor časopisu Tatra Mountains Mathematical Publications (vydavateľstvo Walter de Gruyter).
- **doc. RNDr. Karol Nemoga, PhD.** je výkonným redaktorom slovenskej jednotky časopisu Zentralblatt für Mathematik, Springer-Verlag, Berlin.
- **prof. Dr. Ing. Miloš Oravec** je editorom časopisu Central European Journal of Computer Science (CEJCS), publisher: Versita, co-published with Springer Verlag
- **doc. RNDr. Michal Zajac, PhD.** je výkonným redaktorom časopisu Mathematica Slovaca pre oblasť funkcionálna analýza (vydavateľ MÚ SAV a Springer-Verlag)

### XIV.3. Recenzie pre vedecké časopisy, knihy, zborníky a učebnice

**prof. RNDr. Igor Bock, PhD.** – 1. Mathematics and Mechanics of Solids – 1 recenzia  
 2. Acta Polytechnica Hungarica – 1 recenzia  
 3. Publicationes Mathematicae Debrecen – 1 recenzia  
 4. Discrete and Continuous Dynaical Systems – 1 recenzia  
 5. Mathematical Reviews – 14 prehľadov  
 6. Zentralblatt für Mathematik – 13 prehľadov

**RNDr. Viera Čerňanová, PhD.** – 1. Boletín de la Sociedad Matemática Mexicana-Springer – 1 recenzia

**prof. RNDr. Otokar Grošek, PhD.** – 1. *Searching for Cryptographically Secure Elliptic Curves Over Prime Fields*“, pre časopis Science & Military, 9.3.  
 2. pre CECC '16 - 3 recenzie

**doc. RNDr. Vladimír Olejček, PhD.** – Mathematica Slovaca – 1 recenzia

**doc. RNDr. Michal Zajac, PhD.** – 1. Periodica Mathematica Hungarica -1 recenzia  
 2. Mathematica Slovaca - 1 recenzia  
 3. Czechoslovak Math. J. - 1 recenzia  
 4. Zentralblatt Mathematik – 7 recenzií  
 5. Mathematical Reviews – 3 recenzie

### XIV.4. Recenzie príspevkov na vedecké konferencie

**Mgr. Ing. Matúš Jókay, PhD.:** Sami 2017 – Obfuscation Method Proposal as the Main Tool for Hiding the Malicious software

**RNDr. Igor Brilla, PhD.:** TERCER CONGRESO MULTIDISCIPLINARIO DE CIENCIAS APLICADAS EN LATINOAMÉRICA - COMCAPLA 2016 – 4 recenzie

## **XIV.5. Recenzie vedeckých projektov**

**prof. RNDr. Igor Bock, PhD. – Projekt VEGA – 1 recenzia**

**doc. RNDr. Michal Zajac, PhD. - 1 posudok projektu pre CVTI (podporná schéma na návrat odborníkov zo zahraničia)**

## **XV. ORGANIZÁCIA KONFERENCIÍ**

**NÁZOV KONFERENCIE: Workshop on Secure Implementation of Post-Quantum Cryptography**

**Miesto:** TAU, Izrael

**Dátum:** 26.-27.9.2016

**Meno:** prof. RNDr. Otokar Grošek, PhD.

**Funkcia:** člen organizačného výboru

**NÁZOV KONFERENCIE: TERCER CONGRESO MULTIDISCIPLINARIO DE CIENCIAS APLICADAS EN LATINOAMÉRICA - COMCAPLA 2016**

**Miesto:** Havana

**Dátum:** 6.-9.12.2016

**Meno:** Igor Brilla

**Funkcia:** člen vedeckého výboru

**NÁZOV KONFERENCIE: CECC 2016**

**Miesto:** Piešťany

**Dátum:** 22.-24.6.2016

**Meno:** prof. RNDr. Otokar Grošek, PhD.

**Funkcia:** chair of Session 2

## **XVI. SEMINÁRE**

**Seminár: VARIÁČNÉ NEROVNICE A OPTIMÁLNE RIADENIE V MECHANIKE**

**Vedúci:** prof. RNDr. Igor Bock, PhD.

**Seminár: CRYPTO**

**Vedúci:** doc. Ing. Pavol Zajac, PhD.

**Seminár: MACHINE LEARNING**

**Vedúci:** prof. Dr. Ing. Miloš Oravec

**Seminár: APLIKÁCIE MATEMATIKY**

**vedúci:** doc. RNDr. Oľga Nánásiová, PhD.