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

za rok 2015

riaditeľ ústavu:
prof. RNDr. Otokar Grošek, PhD. Tel: ++421-2-602 91 226
e-mail: otokar.grosek@stuba.sk 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 Kossaczký, CSc. 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.
Výskumní pracovníci	Ing. Csaba Cserba (do 31.8.2015) Ing. Stanislav Marček

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

Interní doktorandi
Ing. Eugen Antal
Ing. Maroš Čavojský
Mgr. Tomáš Fabšič
Ing. Matej Féder (ukončil do 17.4.2015)
Ing. Vojtěch Jirka (prerušené od 1.7.2015)
Ing. Pavol Marák
Ing. Ľuboš Omelina (prerušené do 15.11.2016)
Ing. Alexandra Posoldová (prerušené do 28.8.2016)
Ing. Dominik Sopiak
Ing. Juraj Varga
Mgr. Tomáš Žilka (prerušené do 1.9.2015)
Mgr. Viktória Žilková (rod.Rozborová) (prerušené do 1.9.2015)

Externí doktorandi
Ing. Ján Bédi
Ing. Robert Bučko
Ing. Csaba Cserba (zanechal 7.9.2015)
Ing. Igor Kazlov (od 1.6.2014)
MUDr. Veronika Kurilová (zanechala 7.9.2015)
Mgr. Jozef M. Kollár (prerušené do 30.8.2016)
Ing. Stanislav Marček (prerušené do 30.6.2016)
Ing. Ján Mazanec (zanechal 7.9.2015)
Ing. Ivan Oravec (zanechal 7.9.2015)
Ing. Štefan Počarovský
Ing. Marek Repka (ukončil 25.11.2015)
Ing. Andrej Savka (zanechal 20.7.2015)
Mgr. Zuzana Ševčíková (prerušené do 1.9.2015)
Mgr. Tomáš Žilka (od 1.9.2015)
Mgr. Viktória Žilková (rod.Rozborová) (od 1.9.2015)

II. ZARIADENIA

II.1. Výukové a výskumné laboratóriá

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

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

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

III. VÝUČBA

III.1. Bakalárske štúdium (Bc.)

● Analýza a zložitosť algoritmov (32007)	(6. sem. 3-1 h)	M. Vojvoda
● Analýza a zložitosť algoritmov (B-AZA)	(5. sem. 3-1 h)	M. Vojvoda
●Architektúra softvérových systémov (32022)	(6. sem. 2-2 h)	I. Kossaczký
●Diskrétne udalostné systémy (B-DUS)	(3. sem. 2-2 h)	G.Juhás
●Klasické šifry (32012)	(4. sem. 2-2 h)	O. Grošek
●Klasické šifry (B-KSIF)	(5. sem. 2-2 h)	O. Grošek
●Komunikačné siete 1 (32050)	(4. sem. 3-1 h)	M.Oravec
●Komunikačné siete 2 (35071)	(6. sem. 4-1 h)	A.Hambalík
●Lineárna algebra (31704)	(4. sem. 2-2 h)	M. Zajac
●Lineárna algebra (B-LA)	(3. sem. 2-2 h)	M. Zajac/ I. Marinová/ O. Nánásiová
●Logické systémy op. (34714, 34713, 34711, 34708, 34710, 34712)	(2. sem. 4-1 h)	M. Polakovič
●Manažment IT projektov (B-MITP)	(5. sem. 2-2 h)	O. Malý
●Matematická analýza 1 (MA1_B FIIT)	(1. sem. 4-2 h)	Ľ. Marko/ M. Zákopčan
●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
●Matematika 1 (B-MAT1I)	(1. sem. 3-2 h)	M. Kečkemétyová
●Matematika 1 op. (34706, 34705, 31702, 31701, 31706, 34709)	(2. sem. 4-2 h)	M. Kečkemétyová

●Matematika 2 op. (B-MAT2I, B-MAT2E)	(3. sem. 3-2 h)	V. Olejček
●Matematika 2 (34700)	(2. sem. 4-2 h)	O. Nánásiová/ K. Čipková
●Matematika 2 (34704, 34701, 31708, 34702)	(2. sem. 4-2 h)	I. Brilla/ V. Čerňanová
●Matematika 2 (34703)	(2. sem. 4-2 h)	B. Rudolf
●Matematika 3 (B-MAT3)	(3. sem. 3-2 h)	Ľ. Marko I.Brilla
●Matematika 3 op. (31709, 31712, 31713, 31716)	(4. sem. 3-2 h)	Ľ. Marko
●Matematika 4 (34715, 34716, 34717)	(4. sem. 3-2 h)	V. Olejček/ D. Pancza
●Operačné systémy (B-OS)	(5. sem. 2-2 h)	M. Jókay
●Parciálne diferenciálne rovnice (B-PDR)	(4. sem. 2-2 h)	I. Bock
●Počítačová kriminalita (32011)	(6. sem. 2-2 h)	Š. Balogh
●Pravdepodobnosť a štatistika (PAS_B)	(6. sem. 2-2 h)	V. Olejček
●Programovacie techniky (32019)	(2. sem. 3-2 h)	M. Drozda
●Programovacie techniky (B-PT)	(3. sem. 3-2 h)	M. Drozda
●Projektovanie databázových systémov (32006)	(4. sem. 3-1 h)	I. Kossaczký
●Rýchle algoritmy (32018)	(6. sem. 2-2 h)	K. Nemoga
●Seminár z Matematiky 1	(1. sem. 0-2 h)	B. Rudolf/ M. Kečkemétyová/ M. Zajac
●Seminár z Matematiky 2 (31757)	(2. sem. 0-2 h)	V. Čerňanová/ B. Rudolf/ O. Nánásiová
●Softvérové inžinierstvo (B-SWI)	(5. sem. 2-2 h)	M. Šrámka
●Štatistické metódy v informatike (31719)	(4. sem. 3-2 h)	E. Pastuchová/ I. Marinová
●Teoretické základy informatiky (35033)	(4. sem. 3-2 h)	V. Hromada
●Workflow manažment systémy (32021)	(6. sem. 2-2 h)	P. Frič
●Základy finančníctva (31755)	(2. sem. 1-2 h)	M. Zákopčan

III.2. Inžinierske štúdium (Ing.)

●Analýza a syntéza udalostných systémov (35069)	(2. sem. 3-2 h)	G. Juhás
●Architektúra softvérových systémov (I-ASOS)	(3. sem. 2-2 h)	I. Kossaczký
●Bezpečnosť informačných systémov s pohľadu praxe (35065)	(2. sem. 3-2 h)	M. Šrámka
●Logika (I-LOG)	(1.+3. sem. 3-2 h)	K. Nemoga
●Matematika (34760)	(1. sem. 2-2 h)	I. Bock
●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 šifier (I-NKS)	(3. sem. 2-2 h)	M.Vojvoda/ P.Zajac/ M.Sýs
●Návrh šifrátorov (35037)	(2. sem. 3-2 h)	P. Zajac

●Paralelné programovanie a distribuované systémy (I-PPDS)	(3. sem. 2-2 h)	M. Jókay
●Reprezentácia a získavanie znalostí (I-RZZ)	(1.+3. sem. 2-2 h)	I. Kossaczký
●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.+3. sem. 2-2 h)	M. Oravec
●Systémové programovanie (35060)	(2. sem. 3-2 h)	M. Jókay
●Šifrovanie v komunikačných sieťach (I-SKS)	(1. sem. 3-2 h)	M. Sýs
●Teória fuzzy systémov (31718, 34722)	(1. sem. 3-2 h)	O. Nánásiová
●Teória kódovania (31777, 34778)	(1. sem. 3-1 h)	K. Čipková
●Úvod do počítačovej bezpečnosti (35037)	(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
●Štatistika pre informatikov	O. Grošek
●Teória konečných polí	O. Grošek
●Predmet špecializácie Aplikovaná informatika I	M. Drozda
●Predmet špecializácie Aplikovaná informatika II	M. Drozda
●Teoretické princípy informačných vied- Stochastické modely	V. Olejček
●Teória odboru Aplikovaná informatika	M. Drozda

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

●Analýza a zložitosť algoritmov	M. Vojvoda
●Architektúra počítačov	M. Jókay
●Architektúra softvérových systémov	I. Kossaczký
●Bezpečnosť informačních systémov z pohľadu praxe	M. Šrámka
●Diskrétne udalostné systémy	V. Hromada
●Finančný manažment	M. Zákopčan
●Matematika 1	M. Zajac
●Matematika 2	K. Čipková
●Matematika 3	Ľ. Marko
●Mobilné výpočty	M. Drozda
●Návrh a kryptoanalýza šifier	M. Sýs/ M. Vojvoda
●Návth šifrátorov	P.Zajac
●Logika	K. Nemoga
●Objektovo-orientované programovanie	V. Jirka
●Počítačové siete	J. Varga
●Programovacie techniky	V. Hromada
●Rýchle algoritmy	K. Nemoga
●Spoločenské, morálne a právne súvislosti	M. Šrámka
●Systémové programovanie	M. Jókay
●Vývoj softvérových aplikácií	M. Šrámka

III.5. Dištančné štúdium

●Matematika 2	(2. sem. 6x2h konzul.)	V. Olejček

●Matematika 3	(3. sem. 6x2h konzul.)	Ľ. Marko
●Matematika 4	(4. sem. 6x2h konzul.)	V. Olejček
●Lineárna algebra	(3. sem. 6x2h konzul.)	M. Zajac

IV. VÝSKUMNÉ PROJEKTY

IV.1. Projekty VEGA, ESF, APVV a iné riešené v roku 2015 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 2015: Mgr. Ing. Matúš Jókay, PhD.
Doba riešenia: 2013 - 2016

Číslo projektu: VEGA 1/0173/13
Názov projektu: Ochrana osobných údajov v mobilných zariadeniach
Vedúci projektu: doc. Ing. Pavol Zajac, PhD.
Zástupca vedúceho projektu: doc. Ing. Michal Šrámka, PhD.
Spoluriešitelia z ÚIM v roku 2015: prof. RNDr. Otokar Grošek, PhD., doc. Ing. Milan Vojvoda, PhD., Mgr. Ing. Matúš Jókay, PhD., Ing. Alexander Hambalík, PhD., Ing. Eugen Antal, Ing. Viliam Hromada, PhD., Ing. Pavol Marák, Ing. Juraj Varga, Ing. Štefan Balogh, mgr. Tomáš Fabšič
Doba riešenia: 01.2013-12.2015

Číslo projektu: VEGA 1/0426/12
Názov projektu: Dynamické kontaktné úlohy
Vedúci projektu: prof. RNDr. Igor Bock, PhD.
Zástupca vedúceho projektu: doc. RNDr. Michal Zajac, PhD.
Spoluriešitelia z ÚIM v roku 2015: RNDr. Mária Kečkemétyová, PhD., doc. RNDr. Ľubomír Marko, PhD., Mgr. Dávid Pancza, PhD., doc. Mgr. Marcel Polakovič, PhD., doc, RNDr. Boris Rudolf, PhD., Mgr. Michal Zákopčan, PhD., Mgr. Viktória Žilková, Mgr. Tomáš Žilka
Doba riešenia: 01.2012-21.12.2015

Číslo projektu: OPVV - ITMS kód: 26240220039
Názov projektu: Medzinárodné centrum excelentnosti pre výskum inteligentných a bezpečných informačno-komunikačných technológii a systémov
Spoluriešitelia z ÚIM za rok 2015: prof. RNDr.Otokar Grošek, PhD., doc. RNDr, Karol Nemoga, PhD., doc. Ing. Milan Vojvoda, PhD., Mgr. Ing. Matúš Jókay, PhD., Ing. Viliam Hromada, PhD., Ing. Alexander Hambalík, PhD., prof. Dr. Ing. Miloš Oravec, Ing. Štefan Balogh, PhD., Ing. Ondrej Gallo, PhD., doc. RNDr. Ľubomír Marko, PhD., doc, RNDr. Oľga Nánásiová, PhD.
Doba riešenia: 02/2014-10/2015

Číslo projektu: 2014et018/ Grantový Program nadácie Tatra banky E-Talent 2015
Názov projektu: PinSpace: priestor naokolo je tvoj poznámkový blok
Zodpovedný riesiteľ: Dr. Rer. Nat. Martin Drozda

IV.2. Výskumné úlohy

IV.2.1. Program na podporu mladých výskumníkov

Názov projektu: Návrh multimodálneho biometrického systému
Zodpovedný riešiteľ: Ing. Dominik Sopiak

IV.2.2 Pokračujúce projekty na podporu excelentných mladých výskumníkov

Názov projektu: Rozšírená softvérová extrakcia charakteristických vlastností daktyloskopických vzorov (akronym FingerDetective 2015)
Zodpovedný riešiteľ: Ing. Pavol Marák

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 2015: doc. Ing. Pavol Zajac, PhD., Ing. Marek Repka, Ing, Mgr. Matúš Jókay, PhD., Ing. Ondrej Gallo, PhD., Ing. Juraj Varga, Ing. Eugen Antal, Ing. Viliam Hromada, PhD., Mgr. Tomáš Fabšič, doc. RNDr. Karol Nemoga, PhD.
Doba riešenia: 2012-2015

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 2015: doc. Ing. Pavol Zajac, PhD., Ing. Štefan Balogh, PhD., Mgr. Ing. Matúš Jókay. PhD., Ing. Juraj Varga, Ing. Stanislav Marček, Ing. Maroš Čavojský
Trvanie projektu: 2015-2016

Názov projektu: Kryptografia prináša bezpečnost a slobodu
Číslo projektu: SK06-IV-01-001
Zahraničný partner: Selmenovo centrum, Institutt for Informatikk, Universotetet i Bergen, Nórsko
Vedúci projektu: prof. RNDr. Otokar Grošek, PhD.
Vedúci za nórsku stranu: Tor Helleseth
Riešitelia z ÚIM v roku 2015: 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-0586-11
Názov projektu: Útok na elektronický podpis prostredníctvom analýzy spotreby energie a realizácia protiopatrení
Pracovisko: Katedra elektroniky a multimediálnych telekomunikácií Technickej univerzity v Košiciach
Zodpovedný riešiteľ: Michal Varchola, FEI TUKE
Zástupca vedúceho: prof. RNDr. Otokar Grošek, PhD.
Spoluriešitelia z ÚIM v roku 2015: doc. RNDr. Karol Nemoga, PhD., Ing. Marek Repka, Mgr. Marek Sýs, PhD., doc. Ing. Pavol Zajac, PhD., Ing. Viliam Hromada, PhD., Ing. Eugen Antal
Doba riešenia: 01.7.2012 - 31.12.2015
Dátum oponentúry: 2015

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 2015: prof. RNDr. Igor Bock, PhD.
Doba riešenia: 01.10.2013-30.09.2016

Číslo projektu: OPVaV - ITMS : 26240120037
Názov projektu: Založenie výskumného centra pre analýzu a ochranu dát
Spolupracujúci partner: IBM International Services Centre s.r.o., DWC Slovakia a.s.
Spoluriešitelia v roku 2015 z ÚIM: prof. RNDr. Gabriel Juhás, PhD., prof. Dr. Ing. Miloš Oravec, Dr. rer. nat. Martin Drozda, doc. Ing. Michal Šrámka, PhD.
Doba riešenia: 04/2014 – 09/2015

V. SPOLUPRÁCA

V.1. Domáca spolupráca

V.1.1. Pozvané prednášky

Meno: prof. RNDr. Otokar Grošek, PhD.
Príspevok: Vyznamní "cvoci" sú medzi matematikmi, informatikmi aj psychiatrami
Pozvaná prednáška v rámci medzinárodnej konferencie : V. konferencia o biologickej psychiatrii, Piešťany, 11.-13.6.2015

V.1.2. Spolupráca s domácimi inštitúciami

- Národný bezpečnostný úrad SR, Bratislava
- Kriminalistický 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. Dobrakovová)
- IBM Slovensko, s.r.o.
- WHO kancelária na Slovensku (MUDr. Darina Sedláková)
- Ministerstvo obrany SR

V1.3. Pozvané prednášky domácich odborníkov

Hosť (adresa): Mgr. Juraj Bednár, Citadelo
Termíny: 5.5.2015
Účel: Pozvaná prednáška odborníka z praxe
Prednáška: Kryptomeny

Hosť (adresa): Ing. Ján Václavík, Tatrabanka
Termíny: 8.12.2015
Účel: Pozvaná prednáška odborníka z praxe
Prednáška: Sieťová bezpečnosť

Hosť (adresa): Bc. Martin Orem, Citadelo
Termíny: 15.12.2015
Účel: Pozvaná prednáška odborníka z praxe
Prednáška: Útoky na web aplikácie

V.2. Zahraničná spolupráca

V.2.1. Pozvané prednášky

Meno: Dr.rer.nat. Martin Drozda,
Miesto: National United University, Taiwan
Prednáška: Toward self-aware systems

Meno: Dr.rer.nat. Martin Drozda,
Miesto: Trento, Taliansko
Prednáška: How to detect errors: a personal view
Dátum: 3.-5.6.2015

Meno: Ing. Viliam Hromada, PhD.
Miesto: Tacoma, WA, USA
Prednáška: Fault analysis of stream ciphers
Prednáška: Extracting randomness from mobile devices
Dátum: 14.5.-12.6.2015

Meno: doc.Ing. Pavol Zajac, PhD.
Miesto: Tacoma, WA, USA
Prednáška: Algebraic cryptoanalysis of ciphers with low miltiplicative complexity
Prednáška: Overview of side-channel attacks
Dátum: 28.5.-12.6.2015

NÁZOV KONFERENCIE : *3rd International Conference on Applied Mathematics and Computational Methods (AMCM 2015)*
Miesto: Bratislava
Dátum: 28.-30.11.2015
Meno: RNDr. Igor Brilla, PhD.
Príspevok: Numerical Solution of Boundary Inverse Problems for Plane Orthotropic Elastic Solids

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)
- Prírodovedecká fakulta Masarykovej univerzity v Brne, Brno, Česká republika (doc. Jan Paseka, Mgr. Jiří Janda)
- Matematický ústav AVČR (RNDr. Jiří Jarušek, DrSc., doc. RNDr. Vladimír Müller, DrSc., RNDr. Miroslav Šilhavý DrSc.)
- Ústav informatiky AVČR (prof. RNDr. Štefan Porubský, DrSc.).
- Department of Mathematics, Zhejiang University Hangzhou , Hangzhou & Quzhou, Zhejiang, China (Prof. Junde Wu a jeho doktorandi)
- Oddelenie teoretickej fyziky ,Ústav jadrovej fyziky ČAV, Řež u Prahy, ěská republika (RNDr. Miloslav Znojil, 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)
- Prírodovedecká 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

Hosť (adresa): Martin Fraas, Mathematisches Institut, Universität München
Termín: 18.02.2015
Účel: Pozvaná prednáška v rámci Seminára Variačne nerovnice a optimálne riadenie v mechanike
Prednáška: Hardy weights for a general second order elliptic operator

Hosť (adresa): Tor Helleseth
Termín: 26.-29.5.2015
Účeľ: rokovanie o možnej vedeckej spolupráce a finalizovať podmienky účtovného procesu týkajúce sa projektu

Hosť (adresa): Håvard Raddum
Termín:10.-13.5.2015
Účeľ: rokovanie o finalizácii špecifikácie projektu a potvrdenie dátumov prvej série služobných ciest do Bergenu a Bratislavy.
Pozvaná prednáška: Boolean equations, MRHS equations, CRHS equations

Hosť (adresa): Igor Semaev, Institutt for informatikk, Universitetet i Bergen, Nórsko
Termín: 24.-29.9.2015

Hosť (adresa): Christian Vivelid, Stian Fauskanger, Mohsen Toorani, Asleh Abolpour Mohrad, Tetiana Yarygina, Bjorn Greve, Siddhartha Kumar, Institutt for informatikk, Universitetet i Bergen, Nórsko
Termíny: 9.-13.11.2015
Účel: studijný pobyt v rámci projektu Cryptography brings security amd freedom SK06-IV-01-001

V.2.4. Pobyty pracovníkov ÚIM v zahraničí

Doktorand: Ing. Alexandra Posoldová
Miesto: Austrália

Meno: Ing. Viliam Hromada, PhD.
Miesto: Tacoma, WA, USA
Prednáška: Fault analysis of stream ciphers
Prednáška: Extracting randomness from mobile devices
Dátum: 14.5.-12.6.2015

Meno: doc.Ing. Pavol Zajac, PhD.

Miesto: Tacoma, WA, USA
Prednáška: Algebraic cryptoanalysis of ciphers with low miltiplicative complexity
Prednáška: Overview of side-channel attacks
Dátum: 28.5.-12.6.2015

Meno: Ing. Juraj Varga, Ing. Eugen Antal, Mgr. Tomáš Fabšič,
Miesto: Bergen, Nórsko
Zámer cesty: účast na kryptografickom seminári
Dátum: 22.-26.6.2015

Meno: Ing. Dominik Sopiak
Miesto: Punta Sampieri, Taliansko
Zámer cesty: účast na letnej škole
Dátum: 11.-19.7.2015

Meno: Ing. Maroš Čavojský
Miesto: TU Braunschweig, Nemecko
Zámer cesty: výskum v oblasti Big Data
Dátum: 5.-17.11.2015

V.2.5. Zahraničné cesty

Meno: prof. RNDr. Otokar Grošek, PhD.
Miesto: Londýn, Veľká Británia
Zámer cesty: stretnutie na Real World Cryptography Workshop 2015
Dátum: 7.-9.1.2015

Meno: Dr.rer.nat. Martin Drozda, doc. Ing. Pavol Zajac, PhD., Ing Juraj Varga, Ing. Štefan Balogh, PhD.
Miesto: Bochum, Nemecko
Zámer cesty: pracovné stretbutie na Ruhr Universität
Dátum: 4.-6.3.2015

Meno: doc. Ing. Pavol Zajac, PhD., doc. RNDr. Karol Nemoga, PhD., prof. RNDr. Otokar Grošek, PhD.
Miesto: Tel Aviv, Izrael
Zámer cesty: spolupráca na medzinárodnom projekte-prezentácia výsledkov
Dátum: 2.-7.5.2015

Meno: doc. RNDr. Michal Zajac, PhD.
Miesto: Ľubľana, Slovinsko
Zámer cesty: práca na spoločnom článku s prof. Brančičom
Prednáška: Reflexity and hyperreflexivity of intertwiners
Dátum: 27.5.-1.6.2015

Meno: Dr.rer.nat. Martin Drozda, prof. RNDr. Gabriel Juhás, PhD.
Miesto: Trento, Taliansko
Zámer cesty: stretnutie s profesorom I. Chlamtáčom vo výskumnom pracovisku Create-Net v Trente

Prednáška: How to detect errors: a personal view
Dátum: 3.-5.6.2015

Meno: doc. RNDr. Karol Nemoga, PhD., prof. RNDr. Otokar Grošek, PhD.
Miesto: Bergen, Nórsko
Zámer cesty: práca na spoločnom projekte s univerzitou v Bergene (Cryptography brings security amd freedom SK06-IV-01-001)
Dátum: 22.-27.8.2015

Meno: doc. Ing. Pavol Zajac, PhD.
Miesto: Bergen, Nórsko
Zámer cesty: práca na spoločnom projekte s univerzitou v Bergene (Cryptography brings security amd freedom SK06-IV-01-001)
Dátum: 7.-12.9.2015

Meno: prof. RNDr.Igor Bock, PhD.
Miesto: Praha, ČR
Zámer cesty: Práca na príprave článku do časopisu Nonlinear Analysis na Matematickom ústave akadémie vied ČR
Dátum: 21.-25.10.2015

Meno: prof. RNDr. Gabriel Juhás, PhD.
Miesto: Augsburg/Norimberg, Nemecko
Zámer cesty: výskum a príprava publikácie so zahraničnými partnermi projektu *Založenie výzkumného centra pre analýzu a ochranu dát*
Dátum: 1.-3.11.2015

Meno: doc. RNDr. Michal Zajac, PhD.
Miesto: Varšava, Poľsko
Zámer cesty: účast na seminári Operator Theory seminar na Matematickom ústave polskej akadémie vied
Prednáška: On constants of hyperreflexivity of some spaces of matrices
Dátum: 12.-17.11.2015

V.2.6. Stáže zahraničných pracovníkov na ÚIM FEI STU

V.3. Členstvo v medzinárodných organizáciách a spoločnostiach[1]

[1] 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 Assiociation
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

- **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 členom AMS
- **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. Matej Féder – *Návrh metód extrakcie príznakov a klasifikácie dát v biometrii*, školiteľ prof. Dr. Miloš Oravec, 17.4.2015

Ing. Marek Repka - *Vylepšenie CPA útoku na (EC)DSA a Analýza doby výpočtu McEliece PKC*, školiteľ prof. RNDr. Otokar Grošek, PhD., 25.11.2015

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 doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika na FEI STU.
- **prof. RNDr. Igor Bock, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v študijnom programe 3. stupňa 9.1.9 Aplikovaná matematika so sídlom na FHV ŽU v Žiline
- **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. Igor Bock, PhD.** je členom Vedeckej rady FHV ŽU v Žiline.
- **prof. RNDr. Otokar Grošek, PhD.** je členom Vedeckej rady FEI STU
- **prof. RNDr. Otokar Grošek, PhD.** je podpredsedom 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.

- **prof. RNDr. Gabriel Juhás, PhD.** je predsedom Vedeckej rady 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 dekanom FEI STU
- **prof. RNDr. Gabriel Juhás, PhD.** je členom riadiaceho výboru pre spoluprácu STU Bratislava a ENEL Slovenské elektrárne, a.s.
- **prof. RNDr. Gabriel Juhás, PhD.** Je garantom študijného programu inžinierskeho a doktorandského štúdia Aplikovaná informatika na FEI STU
- **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, Ševčenková 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
- **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 prodekanom FEI STU
- **prof. Dr. Ing. Miloš Oravec** je členom Vedeckej rady FEI STU
- **prof. Dr. Ing. Miloš Oravec** je členom Kolégia dekana FEI STU
- **prof. Dr. Ing. Miloš Oravec** je členom OK študijného programu Aplikovaná informatika na STU
- **prof. Dr. Ing. Miloš Oravec** je spolugarantom študijného programu doktorandského štúdia Aplikovaná informatika na FEI STU
- **prof. Dr. Ing. Miloš Oravec** je člen 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
- **doc. RNDr. Michal Zajac, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU

VII.2. Členstvo v domácich spoločnostiach a organizáciách[2]

- **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
- **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. Peter Volauf, PhD.** je členom JSMF
- **doc. RNDr. Michal Zajac PhD.** je členom JSMF

VII.3. Vedenie prác študentov v súťažiach

VIII. PUBLIKÁCIE

ACB Vysokoškolské učebnice vydané v domácich vydavateľstvách

ACB01 JUHÁS, Gabriel. *Modelling of concurrent systems* [elektronický zdroj /]. 1. ed. Bratislava : Slovak University of Technology, 2015. CD-ROM, 90 s. ISBN 978-80-227-4524-6.

ADC Vedecké práce v zahraničných karentovaných časopisoch

ADC01 NÁNÁSIOVÁ, Oľga - KALINA, Martin. Calculus for Non-Compatible Observables, Construction Through Conditional States. In *International Journal of Theoretical Physics*. Vol. 54, No. 2 (2015), s. 506-518. ISSN 0020-7748. V databáze: WOS: 000349014200015 ; CC ; SCOPUS ; DOI: 10.1007/s10773-014-2243-1.

ADC02 PYKACZ, Jaroslaw - VALÁŠKOVÁ, Ľubica - NÁNÁSIOVÁ, Oľga. Bell-Type Inequalities for Bivariate Maps on Orthomodular Lattices. In *Foundations of Physics*. Vol. 45, no. 8 (2015), s. 900-913. ISSN 0015-9018. V databáze: CC: 000361128800004 ; SCOPUS ; DOI: 10.1007/s10701-015-9906-5.

[2] 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

ADE Vedecké práce v ostatných zahraničných časopisoch

ADE01 JUHÁS, Gabriel - KAZLOV, Igor. Process discovery = Reconstruction of behavior from logs + Model synthesis from behavior. In *Petri Net Newsletter*. Vol. 84, (2015), s. 13-25. ISSN 0391-1804.

ADE02 REPKA, Marek - VARCHOLA, Michal. Correlation Power Analysis using Measured and Simulated Power Traces based on Hamming Distance Power Model - Attacking 16-bit Integer Multiplier in FPGA. In *International Journal of Computer Network and Information Security*. Vol. 7, No. 6 (2015), s. 10-16. ISSN 2074-9104.

ADE03 ZAJAC, Pavol. Impossible differential attacks on 4-round DES-like ciphers. In *International Journal of Computers and Communications*. Vol. 9, (2015), s. 56-61. ISSN 2074-1294.

ADF Vedecké práce v ostatných domácich časopisoch

ADF01 GULÁŠOVÁ, Michala - JÓKAY, Matúš. Steganalysis of stegostorage system. In *Tatra Mountains Mathematical Publications*. Vol. 64, (2015), s. 205-215. ISSN 1210-3195.

ADF02 HROMADA, Viliam - ÖLLÖS, Ladislav - ZAJAC, Pavol. Using sat solvers in large scale distributed algebraic attacks against low entropy keys. In *Tatra Mountains Mathematical Publications*. Vol. 64, (2015), s. 187-203. ISSN 1210-3195.

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

ADM01 ANTAL, Eugen - ZAJAC, Pavol. Key Space and Period of Fialka M-125 Cipher Machine. In *Cryptologia*. Vol. 39, No. 2 (2015), s. 126-144. ISSN 0161-1194. V databáze: WOS: 000353113100003 ; SCOPUS.

ADM02 BRILLA, Igor - JANÍČEK, František. Numerical solution of boundary inverse problems for plane orthotropic elastic solids. In *International Journal of Mechanics*. Vol. 9, (2015), s. 323-328. ISSN 1998-4448. V databáze: SCOPUS: 2-s2.0-84948992627.

ADM03 HROMADA, Viliam - VARGA, Juraj. Phase-shift fault analysis of Trivium. In *Studia Scientiarum Mathematicarum Hungarica*. Vol. 52, No. 2 (2015), s. 205-220. ISSN 0081-6906. V databáze: WOS: 000357757000005.

ADM04 ZAJAC, Pavol. Constructing S-boxes with low multiplicative complexity. In *Studia Scientiarum Mathematicarum Hungarica*. Vol. 52, No. 2 (2015), s. 135-153. ISSN 0081-6906. V databáze: WOS: 000357757000001.

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

ADN01 BOCK, Igor - JARUŠEK, Jiří. A vibrating thermoelastic plate in a contact with an obstacle. In *Tatra Mountains Mathematical Publications*. Vol. 63, (2015), s. 39-52. ISSN 1210-3195. V databáze: SCOPUS: 2-s2.0-84943514301.

ADN02 BOCK, Igor - KEČKEMÉTYOVÁ, Mária. Regularized optimal control problem for a beam vibrating against an elastic foundation. In *Tatra Mountains Mathematical Publications*. Vol. 63, (2015), s. 53-71. ISSN 1210-3195. V databáze: SCOPUS: 2-s2.0-84943525985.

ADN03 BRUNOVSKÝ, Pavol - ZÁKOPČAN, Michal. Equilibria and stable paths in infinite horizon nonlinear control problems: The linear-quadratic approximation. In *Acta Mathematica Universitatis Comenianae*. Vol. 84, No. 1 (2015), s. 79-96. ISSN 0862-9544. V databáze: SCOPUS: 2-s2.0-84922573862.

ADN04 PASTUCHOVÁ, Elena - ZÁKOPČAN, Michal. Comparison of algorithms for fitting a gaussian function used in testing smart sensors. In *Journal of Electrical Engineering*. Vol. 66, No. 3 (2015), s. 178-181. ISSN 1335-3632.

ADN05 REPKA, Marek - VARCHOLA, Michal - DRUTAROVSKÝ, Miloš. Improving CPA attack against DSA and ECDSA. In *Journal of Electrical Engineering*. Vol. 66, No. 3 (2015), s. 159-163. ISSN 1335-3632. V databáze: SCOPUS.

AEC Vedecké práce v zahraničných recenzovaných vedeckých zborníkoch, monografiách

AEC01 ŠRÁMKA, Michal. Evaluating Privacy Risks in Social Networks from the User's Perspective. In *Studies in Computational Intelligence*. Vol. 567 : Advanced Research in Data Privacy, (2015), s. 251-267. ISSN 1860-949X. V databáze: SCOPUS: 2-s2.0-84927127806.

AFA Publikované pozvané príspevky na zahraničných vedeckých konferenciách

AFA01 VARCHOLA, Michal - DRUTAROVSKÝ, Miloš - REPKA, Marek. Robust FPGA based True Random Number Generator utilizing Oscillatory Metastability in Transition Effect Ring Oscillators. In *Advances in Circuits, Systems, Signal Processing and Telecommunications [elektronický zdroj] : Proceedings* : WSEAS, 2015, S. 90-96. ISSN 1790-5117. ISBN 978-1-61804-271-2.

AFC Publikované príspevky na zahraničných vedeckých konferenciách

AFC01 BRILLA, Igor - JANÍČEK, František. Numerical determination of elastic coefficients for orthotropic plates. In *CAIP´2015 [elektronický zdroj] : 12° Congreso interamericano de computación aplicado a la industria de procesos. Cartagena de Indias, Colombia. 14 al 17 de Septiembre de 2015*. Bogotá : Universidad Libre, 2015, CD-ROM, [6] s. ISBN 978-958-8791-82-1.

AFC02 HAMBALÍK, Alexander - MARÁK, Pavol. Image content software analysis. In *Trendy ve vzdělávání*. Roč. 8, č. 1 (2015), s. 71-80. ISSN 1805-8949.

AFC03 JANÍČEK, František - CERMAN, Anton - PERNÝ, Milan - BRILLA, Igor - MARKO, Ľubomír - MOTYČÁK, Štefan. Applications of superconducting quantum interference devices. In *Electric power engineering 2015 : 16th International scientific conference on electric power engineering (EPE). Kouty nad Desnou, Czech Republic. May 20-22, 2015*. Ostrava : VSB - Technical University of Ostrava, 2015, S. 429-432. ISBN 978-1-4673-6787-5. V databáze: SCOPUS: 2-s2.0-84943311844.

AFC04 KURILOVÁ, Veronika - PAVLOVIČOVÁ, Jarmila - ORAVEC, Miloš - RAKÁR, Radoslav - MARČEK, Igor. Retinal blood vessels extraction using morphological operations. In *IWSSIP 2015 : 22nd International conference on systems, signals and image Processing. London, United Kingdom. 10 - 12 September 2015*. London : City University London, 2015, S. 265-268. ISBN 978-1-4673-8352-3.

AFC05 LEHOTA, Ľuboš - ORAVEC, Miloš. Comparison of network traffic classification using single statistical feature versus classification using two features. In *IN-TECH 2015 : Preceedings of the International conference on innovative technologies. Dubrovnik, Croatia. 09.-11.09.2015*. Rijeka : Engineering University of Rijeka, 2015, S. 186-189. ISSN 1849-0662.

AFC06 LODERER, Marek - PAVLOVIČOVÁ, Jarmila - ORAVEC, Miloš - MAZANEC, Ján. Face parts importance in face and expression recognition. In *IWSSIP 2015 : 22nd International conference on systems, signals and image Processing. London, United Kingdom. 10 - 12 September 2015*. London : City University London, 2015, S. 188-191. ISBN 978-1-4673-8352-3.

AFC07 ORAVEC, Miloš - SOPIAK, Dominik - JIRKA, Vojtěch - PAVLOVIČOVÁ, Jarmila - BUDIAK, Mark. Clustering algorithms for face recognition based on client-server architecture. In *IWSSIP 2015 : 22nd International conference on systems, signals and image Processing. London, United Kingdom. 10 - 12 September 2015*. London : City University London, 2015, S. 241-244. ISBN 978-1-4673-8352-3.

AFC08 SÝS, Marek - ŘÍHA, Zdeněk - VASHEK, Matyáš. NIST statistical test suite - result interpretation and optimization. In *Mikulášská kryptobesídka 2015 : sborník příspěvků. Praha, ČR, 3. - 4. 12. 2015*. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2015, S. 14-17. ISBN 978-80-904257-7-4.

AFC09 VARGA, Juraj - GULÁŠOVÁ, Michala - OREM, Martin - DOBROČKA, Pavol - NOVOTNÝ, Daniel - BOLEDOVIČ, Andrej. Mitigating possible threats from overprivileged android applications. In *IN-TECH 2015 : Preceedings of the International conference on innovative technologies. Dubrovnik, Croatia. 09.-11.09.2015*. Rijeka : Engineering University of Rijeka, 2015, S. 42-45. ISSN 1849-0662.

AFC10 VARCHOLA, Michal - DRUTAROVSKÝ, Miloš - ZAJAC, Pavol - REPKA, Marek. Side Channel Attack on Multiprecision Multiplier Used in Protected ECDSA Implementation. In *ReConFig 2015 : 2015 International conference on ReConFigurable computing and FPGAs. Mayan Riviera, Mexico, December 7-9, 2015*. [s.l.] : IEEE, 2015, on-line, [6] s. V databáze: IEEE.

AFD Publikované príspevky na domácich vedeckých konferenciách

AFD01 BOCK, Igor - JARUŠEK, Jiří - ŠILHAVÝ, Miroslav. On an acceleration term in a dynamic contact of plates with a rigid obstacle. In *10th Workshop on functional analysis and its applications in mathematical physics and optimal control [Kočovce, Slovak Republic. September 7-12, 2015 /]*. 1. vyd. Bratislava : STU v Bratislave, 2015, S. 7-11. ISBN 978-80-227-4411-9.

AFD02 BOCK, Igor. Dynamic contact of beams with rigid obstacles. In *New Trends in Statics and Dynamics of Buildings [elektronický zdroj] : proceedings of 13th International Conference. Bratislava, Slovakia, 15. - 16. 10. 2015*. 1. vyd. Bratislava : Slovak University of Technology in Bratislava, 2015, CD-ROM, [6] s. ISBN 978-80-227-4463-8.

AFD03 JUHÁS, Gabriel - KISELICOVÁ, Renáta - MOLNÁR, Ľ. Postdraduate development: an intriguing journey from a graduate to the IT professional. In *ICETA 2015 : 13th IEEE international conference on emerging eLearning technologies and applications. Starý Smokovec, Slovakia. November 26 - 27, 2015*. Danvers : IEEE, 2015, S. 177-182. ISBN 978-1-4673-8534-3.

AFD04 KEČKEMÉTYOVÁ, Mária - BOCK, Igor. Regularized optimal control problem for an anisotropic plate vibrating against an elastic foundation. In *10th Workshop on functional analysis and its applications in mathematical physics and optimal control [Kočovce, Slovak Republic. September 7-12, 2015 /]*. 1. vyd. Bratislava : STU v Bratislave, 2015, S. 18-23. ISBN 978-80-227-4411-9.

AFD05 KEČKEMÉTYOVÁ, Mária - BOCK, Igor. An optimal design problem for a Mindlin-Timoshenko beam vibrating against an elastic foundation. In *New Trends in Statics and Dynamics of Buildings [elektronický zdroj] : proceedings of 13th International Conference. Bratislava, Slovakia, 15. - 16. 10. 2015*. 1. vyd. Bratislava : Slovak University of Technology in Bratislava, 2015, CD-ROM, [4] s. ISBN 978-80-227-4463-8.

AFD06 MARKO, Ľubomír. Thickness optimization of a dynamic axisymmetric circular plate on an elastic foundation. In *New Trends in Statics and Dynamics of Buildings [elektronický zdroj] : proceedings of 13th International Conference. Bratislava, Slovakia, 15. - 16. 10. 2015*. 1. vyd. Bratislava : Slovak University of Technology in Bratislava, 2015, CD-ROM, [4] s. ISBN 978-80-227-4463-8.

AFD07 ORAVEC, Miloš - SOPIAK, Dominik - JIRKA, Vojtěch. Face recognition on mobile devices based on client-server architecture. In *Redžúr 2015 [elektronický zdroj] : 9th International workshop on multimedia and signal processing. Smolenice, Slovakia. April 22-23, 2015*. 1. vyd. Bratislava : Nakladateľstvo STU, 2015, S. 15-18. ISBN 978-80-227-4346-4.

AFD08 PANCZA, Dávid - BOCK, Igor. Dynamic contact of Mindlin-Timoshenko beam with a rigid obstacle. In *New Trends in Statics and Dynamics of Buildings [elektronický zdroj] : proceedings of 13th International Conference. Bratislava, Slovakia, 15. - 16. 10. 2015*. 1. vyd. Bratislava : Slovak University of Technology in Bratislava, 2015, CD-ROM, [7] s. ISBN 978-80-227-4463-8.

AFD09 POLAKOVIČ, Marcel. D-weak operator topology and some its properties. In *10th Workshop on functional analysis and its applications in mathematical physics and optimal control [Kočovce, Slovak Republic. September 7-12, 2015 /]*. 1. vyd. Bratislava : STU v Bratislave, 2015, S. 46-47. ISBN 978-80-227-4411-9.

AFD10 POSOLDOVÁ, Alexandra - LIEW, Alan - RYBÁROVÁ, Renáta. Content based rating prediction recommendation system for HBB TV. In *Redžúr 2015 [elektronický zdroj] : 9th International workshop on multimedia and signal processing. Smolenice, Slovakia. April 22-23, 2015*. 1. vyd. Bratislava : Nakladateľstvo STU, 2015, S. 79-82. ISBN 978-80-227-4346-4.

AFD11 RUDOLF, Boris. On the landesman-lazer condition for three point boundary value problem at resonance. In *10th Workshop on functional analysis and its applications in mathematical physics and optimal control [Kočovce, Slovak Republic. September 7-12, 2015 /]*. 1. vyd. Bratislava : STU v Bratislave, 2015, S. 48-50. ISBN 978-80-227-4411-9.

AFD12 ZAJAC, Michal. Examples of morphisms of operator effect algebras. In *10th Workshop on functional analysis and its applications in mathematical physics and optimal control [Kočovce, Slovak Republic. September 7-12, 2015 /]*. 1. vyd. Bratislava : STU v Bratislave, 2015, S. 57-58. ISBN 978-80-227-4411-9.

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

BFA01 FABŠIČ, Tomáš - GROŠEK, Otokar - NEMOGA, Karol - ZAJAC, Pavol. On constructing invertible circulant binary(n x n)-matrices with n2/2 ones. In *CECC 2015 : Book of abstracts: 15th Central European conference on cryptology. Klagenfurt am Wörthersee, Austria. July 8-10, 2015*. Vienna : Alpen-Adria-Universität Klagenfurt, 2015, S. 10-12.

BFA02 GULÁŠOVÁ, Michala - JÓKAY, Matúš. Steganalysis of stegostorage system. In *CECC 2015 : Book of abstracts: 15th Central European conference on cryptology. Klagenfurt am Wörthersee, Austria. July 8-10, 2015*. Vienna : Alpen-Adria-Universität Klagenfurt, 2015, S. 17-18.

BFA03 ZAJAC, Pavol - HROMADA, Viliam - ÖLLÖS, Ladislav. A few notes on algebraic cryptanalysis. In *CECC 2015 : Book of abstracts: 15th Central European conference on cryptology. Klagenfurt am Wörthersee, Austria. July 8-10, 2015*. Vienna : Alpen-Adria-Universität Klagenfurt, 2015, S. 44-45.

BFA04 ZAJAC, Pavol. On algebraic cryptanalysis of ciphers with low multiplicative complexity. In *WCC 2015 : 9th International workshop on coding and cryptography. Paris, France. April 13-17, 2015*. Paris : INRIA, 2015, [9] s.

DAI Dizertačné a habilitačné práce

DAI01 FÉDER, Matej. *Návrh metód extrakcie príznakov a klasifikácie dát v biometrii : Dát. obhaj.: 17.4.2015*. Bratislava : FEI STU, 2015. Dostupné na internete: <http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=81779>.

DAI02 REPKA, Marek. *Vylepšenie CPA útoku na (EC)DSA a Analýza doby výpočtu McEliece PKC : dát. obhaj. 25.11.2015, č. ved. odb. 9-2-9*. Bratislava : FEI STU, 2015. 80 s. Dostupné na internete: <http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=104770>.

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

FAI01 ZAJAC, Michal (ed.) - BOCK, Igor (ed.). *10th Workshop on functional analysis and its applications in mathematical physics and optimal control :* [Kočovce, Slovak Republic. September 7-12, 2015 /]. 1. vyd. Bratislava : STU v Bratislave, 2015. 60 s. ISBN 978-80-227-4411-9.

GII Rôzne publikácie a dokumenty, ktoré nemožno zaradiť do žiadnej z predchádzajúcich kategórií

GII01 GROŠEK, Otokar. Prvý v rade. In *Obzory matematiky, fyziky a informatiky*. Roč. 44, č. 2 (2015), s. 39-40. ISSN 1335-4981.

IX. VÝCHOVA VEDECKÝCH PRACOVNÍKOV

IX.1. Interní doktorandi

Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Školiteľ špecialista: Mgr. Marek Sýs, PhD.
Doktorand: Ing. Eugen Antal
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 5.6.2013
Predpokladaný termín ukončenia: 2016
Téma práce: Moderná kryptoanalýza klasických šifier

Školiteľ: Dr.rer.nat. Martin Drozda
Doktorand: Ing. Maroš Čavojský
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Predpokladaný termín ukončenia: 31.5.2017
Téma práce: Metodológia a systém na efektívne testovanie mobilných aplikácií

Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Doktorand: Mgr. Tomáš Fabšič
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 30.9.2015
Predpokladaný termín ukončenia: 31.8. 2016
Prerušenie: 1.2.-2.9.2014
Téma práce: Postranné kanály

Školiteľ: prof. Dr. Ing. Miloš Oravec
Doktorand: Ing. Matej Féder
Forma vzdelávania: doktorandské – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.2.2012

Predpokladaný termín ukončenia: 30.8.2013
Prerušenie: 1.9.2013-1.4.2015
Ukončenie: 17.4.2015
Téma práce: 1.9.2013-1.4.2015

Školiteľ: prof. Dr. Ing. Miloš Oravec
Doktorand: Ing. Vojtěch Jirka
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 tvárí v neriadených podmienkach využitím metód strojového učenia

Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Školiteľ špecialista: Ing. Alexander Hambalík, PhD.
Doktorand: Ing. Pavol Marák
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM**,** FEI STU
Dizertačná skúška: 25.4.2015
Predpokladaný termín ukončenia: 31.8.2015
Téma práce: Charakteristické vlastnosti odtlačkov prstov a dlaní a ich automatické rozpoznávanie

Školiteľ: prof. Dr. Ing. Miloš Oravec
Doktorand: Ing. Ľuboš Omelina
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.2.2011
Predpokladaný termín ukončenia: 2013
Prerušenie: 1.11.2011-31.1.2013 a 15.11.2015-15.11.2016
Téma práce : Návrh metód rozpoznávania vzorov v biometrii

Školiteľ: prof. Dr. Ing. Miloš Oravec
Doktorand: Ing. Alexandra Posoldová
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

Školiteľ: prof. Dr. Ing. Miloš Oravec
Doktorand: Ing. Dominik Sopiak

Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Predpokladaný termín ukončenia: 31.5.2017
Téma práce: Návrh multimodálneho biometrického systému

Školiteľ: doc. Ing. Pavol Zajac, PhD.
Doktorand: Ing. Juraj Varga
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 14.6.2013
Predpokladaný termín ukončenia: 05.9.2015
Téma práce: Bezpečnosť mobilných zariadení.

Školiteľ: prof. RNDr. Igor Bock, PhD.
Doktorand: Mgr. Tomáš Žilka
Prijatý dňa: 8.7.2010
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: 9.1.9 Aplikovaná matematika
Pracovisko: OM ÚIM FEI STU v Bratislave
Dátum dizertačnej skúšky: 28.2.2012
Predpokladaný termín ukončenia: 28.8.2014
Prerušenie: 1.9.2014-1.9.2015
Téma práce: Dynamický kontakt dosky s prekážkou

Školiteľ: doc. RNDr. Michal Zajac, PhD.
Doktorand: Mgr. Viktória Žilková (rod. Rozborová)
Prijatá dňa: 8.7.2010
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: 9.1.9 Aplikovaná matematika
Pracovisko: OM ÚIM FEI STU v Bratislave
Dátum dizertačnej skúšky: 28.2.2012
Predpokladaný termín ukončenia: 28.8.2014
Prerušenie: 1.9.2014-1.9.2015
Téma práce: Hyperreflexívnosť priestorov lineárnych operátorov

IX.2. Externí doktorandi

Školiteľ: prof. Dr. Ing. Miloš Oravec
Doktorand: Ing. Ján Bédi
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: 31.8.2014
Predpokladaný termín ukončenia: 31.8.2017
Téma práce: Podpora diagnostikovania v medicíne využitím metód strojového učenia

Školiteľ: doc. RNDr. Jaroslav Fogel, PhD.

Doktorand: Ing. Robert Bučko
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

Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Csaba Cserba
Forma vzdelávania: doktorandské štúdium – externá forma od 1.9.2014, interná forma do 31.8.2014
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Predpokladaný termín ukončenia: 31.5.2017
Téma práce: Metodológia a systém na efektívne testovanie mobilných aplikácií
Vyradenie: 7.9.2015

Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Igor Kazlov
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

Školiteľ: prof. Dr. Ing. Miloš Oravec
Doktorand: MUDr.Veronika Kurilová (rod. Hanúsková)
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: 29.4.2014
Predpokladaný termín ukončenia: 31.8.2015
Téma práce: Nové metódy diagnostiky v oftalmológii
Vyradenie: 7.9.2015

Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Doktorand: Mgr. Jozef Kollár
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

Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Stanislav Marček
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
Predpokladaný termín ukončenia: august 2014
Téma práce: Modelovanie a simulácia udalostných systémov

Školiteľ: prof. Dr. Ing. Miloš Oravec
Doktorand: Ing. Ján Mazanec
Forma vzdelávania: doktorandské štúdium – externá forma od 1.9.2014, interná forma do 31.8.2014
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 12.11.2009
Predpokladaný termín ukončenia: 2013
Téma práce: Rozpoznávanie tvárí a tvárových čŕt
Vyradenie: 7.9.2015

Školiteľ: doc. Ing. Michal Šrámka, PhD.
Doktorand: Ing. Ivan Oravec
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: jún 2015
Predpokladaný termín ukončenia: jún 2018
Téma práce: Ochrana osobných údajov v mobilných zariadeniach

Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Štefan Počarovský
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: 19.3.2014
Predpokladaný termín ukončenia: 01.5.2013
Téma práce: Virtualizácia elektronických služieb

Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Martin Rástocký
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška:
Predpokladaný termín ukončenia: 05.9.2016
Vyradenie: 1.9.2014
Téma práce: Workflow manažment systémy a manažment zmien udalostných procesov

Školiteľ: prof. RNDr. Otokar Grošek, PhD.

Doktorand: Ing. Marek Repka
Forma vzdelávania: doktorandské štúdium – externá forma od 1.11.2012, interná od 1.9.2010 do 1.11.2012
Odbor: Aplikovaná informatika
Pracovisko: ÚIM,FEI STU
Dizertačná skúška: 28.2.2012
Predpokladaný termín ukončenia: 30.8.2013
Ukončenie: 25.11.2015
Téma práce: Post-kvantová kryptografia

Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Andrej Savka
Forma vzdelávania: doktorandské štúdium – externá forma od 1.9.2012, interné od 1.9.2011 do 1.9.2012
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.2.2013
Predpokladaný termín ukončenia: 05.9.2014
Zanechanie štúdia: 20.7.2015
Téma práce: Workflow manažment systémy a manažment zmien udalostných systémov

Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Doktorand: Mgr. Zuzana Ševčíková
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

Školiteľ: prof. RNDr. Igor Bock, PhD.
Doktorand: Mgr. Tomáš Žilka
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

Školiteľ: doc. RNDr. Michal Zajac, PhD.
Doktorand: Mgr. Viktória Žilková (rod. Rozborová)
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

X. ÚČASŤ PRACOVNÍKOV ÚSTAVU NA KONFERENCIÁCH

X.1. Zahraničné konferencie

NÁZOV KONFERENCIE : The Ninth international Workshop on Coding and Cryptography 2015
Miesto: Paríž, Francúzsko
Dátum: 12.-17.4.2015
Meno: doc. Ing. Pavol Zajac, PhD.
Príspevok: On algebraic cryptanalysis of ciphers with low multiplicative complexity

NÁZOV KONFERENCIE : Mediterranean Conference on Information & Communacation Technologies 2015 (MedICT 2015)
Miesto: Saidia, Maroko
Dátum: 7.-9.5.2015
Meno: Ing. Stanislav Marček, Dr.rer.nat. Martin Drozda
Príspevok: Predicting System Failures on Mobile Devices

NÁZOV KONFERENCIE : 36th IEEE symposium and workshop on security and privacy
Miesto: San Jose, USA
Dátum: 16.-24.5.2015
Meno: doc. Ing. Michal Šrámka, PhD., PhD.

NÁZOV KONFERENCIE : Trendy ve vzdělávání
Miesto: Olomouc, Česká republika
Dátum: 17.-19.6.2015
Meno: Ing. Alexander Hambalík, PhD.
Príspevok: Image conetent software analysis

NÁZOV KONFERENCIE : 27. medzinárodná konferencia IFIP TC7
Miesto: Sophia Antipolis, Francúzsko
Dátum: 28.6.-3.7.2015
Meno: prof. RNDr. Igor Bock, PhD.
Príspevok: Regularized optimal design problém for a viscoelastic plate vibrating against a ridig obstacle

NÁZOV KONFERENCIE : 9. konferencia European solid mechanics conference
Miesto: Madrid, Španielsko
Dátum: 6.-11.7.2015
Meno: prof. RNDr. Igor Bock, PhD.
Príspevok: Regularized optimal design problém for a viscoelastic plate vibrating against an elactic foundations

NÁZOV KONFERENCIE : 15th Central european Conference on Cryptology CECC 2015
Miesto: Klagenfurt, Rakúsko
Dátum: 7.-11.7.2015

Meno: doc. Ing. Pavol Zajac, PhD.
Príspevok: A few notes on algebraic crypanalysis

NÁZOV KONFERENCIE : 15th Central european Conference on Cryptology CECC 2015
Miesto: Klagenfurt, Rakúsko
Dátum: 7.-11.7.2015
Meno: Ing. Eugen Antal

NÁZOV KONFERENCIE : 15th Central european Conference on Cryptology CECC 2015
Miesto: Klagenfurt, Rakúsko
Dátum: 7.-11.7.2015
Meno: Mgr. Tomáš Fabšič
Príspevok: On constructing invertible circulant binary (n*n)-matrices with (n^2)/2 ones

NÁZOV KONFERENCIE : 15th Central european Conference on Cryptology CECC 2015
Miesto: Klagenfurt, Rakúsko
Dátum: 7.-11.7.2015
Meno: prof. RNDr. Otokar Grošek, PhD.

NÁZOV KONFERENCIE : The 21st Annual International Conference on Mobile Computing and Networking ***MobiCom 2015***
Miesto: Paríž, Francúzsko
Dátum: 7.-11.9.2015
Meno: Ing. Stanislav Marček, Dr.rer.nat. Martin Drozda, Ing. Maroš Čavojský

NÁZOV KONFERENCIE : 7th European Academy of Forensic Science Conference
Miesto: Praha, Česko
Dátum: 6.-11. 9. 2015
Meno: Ing. Pavol Marák
Príspevok: A Novel Approach to Construction of Statistical Model of Fingerprint Individuality

NÁZOV KONFERENCIE : International Conference on Innovative Technologies IN-TECH 2015
Miesto: Dubrovník, Chorvátsko
Dátum: 8.-13.9.2015
Meno: Ing. Juraj Varga
Príspevok: Mitigating Possible Threats From Overprivileged Android Applications

NÁZOV KONFERENCIE : CAIP 2015 - 12° Congreso Interamericano de Computación Aplicada a la Ingenieria de Procesos
Miesto: Cartagena , Kolumbia
Dátum: 14.9. – 17.9.2015
Meno: RNDr. Igor Brilla, CSc.
Príspevok: Numerical Determination of Elastic Coefficients for Orthotropic Plates

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2015
Miesto: Praha, Česká republika
Dátum: 2.-4.12.2015

Meno: doc. Ing. Pavol Zajac, PhD.
Príspevok: CECC16

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2015
Miesto: Praha, Česká republika
Dátum: 2.-4.12.2015
Meno: Ing. Eugen Antal

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2015
Miesto: Praha, Česká republika
Dátum: 2.-4.12.2015
Meno: Mgr. Ing. Matúš Jókay, PhD.

NÁZOV KONFERENCIE : IEEE SocialCom 2015
Miesto: Chengdu, Čína
Dátum: 19.-21.12.2015
Meno: Dr.rer.nat. Martin Drozda, Ing. Maroš Čavojský

X.2. Domáce konferencie

NÁZOV KONFERENCIE : 12th International Forensic Symposium
Miesto: Bratislava, Slovensko
Dátum: 17.-20. 2. 2015
Meno: Ing. Pavol Marák
Príspevok: A Novel Approach to Construction of Statistical Model of Fingerprint Individuality

NÁZOV KONFERENCIE : V. konferencia o biologickej psychiatrii
Miesto: Piešťany
Dátum: 11.-13.6.2015
Meno: prof. RNDr. Otokar Grošek, PhD.
Príspevok: Vyznamní "cvoci" sú medzi matematikmi, informatikmi aj psychiatrami

NÁZOV KONFERENCIE : 10th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control
Miesto: Kočovce
Dátum: 7.-12.9.2015
Meno: prof. RNDr. Igor Bock, PhD.
Príspevok: On an acceleration term in a dynamic contact of plates with a rigid obstacle
Príspevok: Regularized optimal control problem for an anisotronic plate vibrating against an elastic foundation

NÁZOV KONFERENCIE : 10th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control
Miesto: Kočovce
Dátum: 7.-12.9.2015
Meno: doc. RNDr. Michal Zajac, PhD.
Príspevok: Examples of morphisms of operator effect algebras

NÁZOV KONFERENCIE : 10th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control
Miesto: Kočovce
Dátum: 7.-12.9.2015
Meno: doc. RNDr. Boris Rudolf, PhD.
Príspevok: On the landesman-lazer condition for three point boundary value problem at resonance

NÁZOV KONFERENCIE : 10th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control
Miesto: Kočovce
Dátum: 7.-12.9.2015
Meno: doc. Mgr. Marcel Polakovič, PhD.
Príspevok: D-weak operator topology and some its properties

NÁZOV KONFERENCIE : 10th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control
Miesto: Kočovce
Dátum: 7.-12.9.2015
Meno: RNDr. Mária Kečkemétyová, PhD.
Príspevok: Regularized optimal control problem for an anisotronic plate vibrating against an elastic foundation

NÁZOV KONFERENCIE : *13. medzinárodná konferencia New Trends in Statics and Dynamics of Buildings*
Miesto: Bratislava
Dátum: 15.-16.10.2015
Meno: prof. RNDr. Igor Bock, PhD.
Príspevok: Dynamic contacts of beams with rigid obstacles

NÁZOV KONFERENCIE : *13. medzinárodná konferencia New Trends in Statics and Dynamics of Buildings*
Miesto: Bratislava
Dátum: 15.-16.10.2015
Meno: doc. RNDr. Ľubomír Marko, CSc.
Príspevok: Thickness optimization of a dynamic axisymmetric circular plate on an elastic foundation

NÁZOV KONFERENCIE : *13. medzinárodná konferencia New Trends in Statics and Dynamics of Buildings*
Miesto: Bratislava
Dátum: 15.-16.10.2015
Meno: RNDr. Mária Kečkemétyová, PhD.
Príspevok: An optimal design problém for a Mindlin-Timoshenko beam vibrating against an elastic foundation

NÁZOV KONFERENCIE : *13. medzinárodná konferencia New Trends in Statics and Dynamics of Buildings*
Miesto: Bratislava
Dátum: 15.-16.10.2015

Meno: Mgr. Dávid Pancza, PhD.
Príspevok: Dynamic contacts of Mindlin-Timoshenko beams with rigid obstracles

NÁZOV KONFERENCIE : *13th International Conference on Emerging eLearning Technologies and Applications (ICETA 2015)*
Miesto: Starý Smokovec
Dátum: 26.-27.11.2015
Meno: prof. RNDr. Gabriel Juhás, PhD.
NÁZOV KONFERENCIE : *3rd International Conference on Applied Mathematics and Computational Methods (AMCM 2015)*
Miesto: Bratislava
Dátum: 28.-30.11.2015
Meno: RNDr. Igor Brilla, PhD.
Príspevok: Numerical Solution of Boundary Inverse Problems for Plane Orthotropic Elastic Solids

XI. HABILITAČNÉ A INAUGURAČNÉ KONANIA

XI.1. Inauguračné konania

XI.2. Habilitačné konania

XI.3. Členstvá v komisiách

prof. RNDr.Igor Bock, PhD. – člen habilitačnej komisie RNDr.Boženy Dorociakovej, PhD. FPV UMB v Banskej Bystrici, 2.3.2015

prof. RNDr.Igor Bock, PhD. – člen habilitačnej komisie Mgr.Pavla Bokesa, PhD. FMFI UK v Bratislave, 23.11.2015

doc. RNDr. Boris Rudolf, CSc. - oponent a člen habilitačnej komisie Mgr. Pavla Bokesa, PhD. s názvom Modelling gene expression at low copy numbers, FMFI UK, 23.11.2015

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

XII.1. Obhajoby dizertačnej práce na ÚIM

prof. RNDr. Otokar Grošek, PhD.- predseda komisie obhajoby dizertačnej práce Ing. Mateja Fédera, 17.4.2015

XII.2. Dizertačné skúšky na ÚIM

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

prof. RNDr. Igor Bock, PhD. - člen komisie pre dizertačnú skúšku Ing.Jozefa Urbána, Stavebná fak. STU, 24.8.2015

prof. RNDr. Igor Bock, PhD. - člen komisie na obhajobu dizertačnej práce Ing. Róberta Špiru s názvom *Parallel algorithms for the solution of partial differential equations-Numerical methods for analysis of embryogenesis images* a Ing. Daniela Szatmáriho s názvom *Tvorba a optimalizácia kartografického zobrazenia* a Ing. Michala Smíšeka s názvom *Analysis of 3D a 4D images of organisms in embryogenesis,* SvF STU, 24.8.2015

prof. RNDr. Otokar Grošek, PhD.- člen komisie dizertačnej skúšky Ing. Tibora Csoku z ÚT FEI STU, 16.1.2015

doc. RNDr. Ľubomír Marko, PhD. - člen komisie na obhajobu dizertačnej práce Ing. Róberta Špiru s názvom *Parallel algorithms for the solution of partial differential equations-Numerical methods for analysis of embryogenesis images* a Ing. Daniela Szatmáriho s názvom *Tvorba a optimalizácia kartografického zobrazenia* a Ing. Michala Smíšeka s názvom *Analysis of 3D a 4D images of organisms in embryogenesis,* SvF STU, 24.8.2015

XII.4. Oponentské posudky k dizertačnej práci

prof. RNDr. Igor Bock, PhD. – oponent dizertačnej práce Mgr. Jozefa Mináraa s názvom *Numerical Modelling of Direct and Inverse Problems for Infiltration and Transport in Porous Medium,* FMFI UK, 25.8.2015

prof. RNDr. Igor Bock, PhD. – oponent dizertačnej práce Mgr. Júliusa Pačutu s názvom *A Priori Estimates of Solutions of Superlinear Elliptic and Parabolic Problems,* FMFI UK, 25.8.2015

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

prof. RNDr. Igor Bock, PhD. – oponent písomnej práce k dizertačnej skúške Mgr. Lukáša Tomeka s názvom *Discrete Duality Finite Volume Method for Mean Curvature Flow on Surface ,* Stavebná fak. STU, 24.8.2015

XII.6. Skúšky z matematických predmetov doktorandského štúdia

Meno doktoranda	Odbor štúdia	Meno skúšajúceho	Predmet	Dátum
Peter Balko	Mechatronické systémy	I. Bock	Matematika pre doktorandov	9.1.2015
Alojz Gomola	Mechatronické systémy	I. Bock	Matematika pre doktorandov	23.1.2015
Michal Hanic	Mikroelektronika	I. Bock	Matematika pre doktorandov	5.2.2015
Vladimír Popelka	Automatizácia	I. Bock	Matematika pre doktorandov	10.2.2015
Jozef Daňo	Silnoprúdová elektrotechnika	I. Bock	Matematika pre doktorandov	10.2.2015

Ondrej Kaššák	FIIT	V. Olejček	Stochastické modely	2.7.2015
Martin Konôpka	FIIT	V. Olejček	Stochastické modely	16.7.2015
Peter Laurinec	FIIT	V. Olejček	Stochastické modely	2.7.2015
Marek Lóderer	FIIT	V. Olejček	Stochastické modely	2.7.2015
Jakub Ševcech	FIIT	V. Olejček	Stochastické modely	16.7.2015

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

XIII.1. ŠVOČ

Meno: prof. RNDr. Igor Bock, PhD.
Predseda komisie pre posúdenie prác Študentskej vedeckej konferencie na Staveb. Fak. STU v sekcii Matematicko-počítačové modelovanie, 21.4.2015

XIII.2. VEDENIE UKONČENÝCH DIPLOMOVÝCH PRÁC

Balogh Ľubomír: Paralelné výpočty pomocou FPGA (O. Gallo)

Čajkovič Peter: Monitorovacia stanica rádioaktivity v oblasti Bratislava - Mlynská dolina (K. Vitázek)

Černá Alena: Dekódery pre BCH kódy (K. Nemoga)

Drobec Ján: Webová aplikácia s Petriho sieťami na pozadí (S. Marček)

Gedaj Matúš: Vplyv stresu a hudby na vodiča a riadenie automobilu (M. Kukučka)

Gulyás Andrej: Implementácia QC-MDPC McEliecovho kryptosystému (P. Zajac)

Guzmický Martin: Kompozičná konštrukcia S-boxov (P. Zajac)

Hýl Peter: Ochrana vlastníckych práv v hudbe (O. Grošek, konzultant J. Šiška)

Charvát Juraj: Bezpečnosť platobných systémov budúcnosti (O. Grošek, konzultant J. Šiška)

Jarinčík Peter: Systém pre overovanie identity používateľa pomocou kontextovej informácie (M. Drozda)

Jašura Patrik: Mobilný systém pre nepočujúcich (I. Kazlov)

Kaničár Martin: Kryptoanalýza lightwieght prúdovej šifry WG-8 (V. Hromada)

Khandl Tomáš: Návrh steganografického úložiska vo videu (M. Jókay)

Klein Marek: Postranné kanály v SW implementácii McElieceovho kryptosystému (P. Zajac)

Koma Tibor: Spravovanie prostriedkov vo virtualizačných systémoch pomocou hypervízora Xen (C. Cserba)

Kolimár Ondrej: Multikriteriálne a multivariantné rozhodovanie v prostredí sociálnych sietí (Š. Kozák)

Kósa Péter: Vytvorenie webovej aplikacie na správu hypervízora XEN (C. Cserba)

Kudláč Jozef: Analýza RSA kľúčov v slovenských SSL certifikátoch (M. Šrámka)

Kušnirák Kamil: Poskytovanie geopriestorových údajov prostredníctvom WFS štandardu (O. Gallo)

Leitner Andrej: Poradný systém v športovej analytike (M.Jókay)

Ližičiar Michal: Anonymizačný modul pre Firefox (M. Jókay)

Mach Roman: Individualizované nastavovanie sieťového rozhrania prehliadača Firefox (M. Jókay)

Machovec Filip: Stegoanalýza BPCS (M. Vojvoda)

Maláč Miroslav: Refaktorizácia zásuvného modulu pre UML diagramy (M. Polakovič)

Maras František: Riadenie laboratórneho experimentu v prostredí Internetu (K. Žáková)

Matúš Markusek: Využívanie publikačných internetových informačných zdrojov pre tvorbu citačného indexu (K. Žáková)

Molnár Gábor: Pokročilé metódy 3D rekonštrukcie (M. Sýs)

Nižnanská Miriama: Aplikácia na editovanie a softvérovú podporu hybridných Petriho sietí (D. Rosinová)

Novák Jakub: Získanie vhodného riešenia syntézy Petriho sietí (C. Cserba)

Ondrejkovič Matúš: Modul pre virtuálne a vzdialené laboratória v systéme Moodle (P. Bisták)

Papson Boris: Získavanie údajov z mobilných senzorov (S. Marček)

Paučo Martin: Modelovanie automatizovaných skladových systémov pomocou Petriho sietí (A. Kozáková)

Prichocká Michaela: Využitie neurónových sietí na hodnotenie kvality zvarov (A. Kozáková)

Rakár Radoslav: Segmentácia významných oblastí na obrazoch sietnice (J. Pavlovičová)

Regenda Patrik: Aplikácie konkurentné, distribuované a odolné voči chybám v kontexte dávkového spracovania dát (I. Kossaczký)

Rýznar Karol: Platobné systémy v mobilných zariadeniach (M. Šrámka)

Sabo Miroslav: Systém pre vzdialenú editáciu a vyhodnocovanie programov v jazyku Java (M. Polakovič)

Szabo Tomáš: Aplikácia na tvorbu interaktívnych animácii pre internetové prehliadače (M. Polakovič)

Šlezinger Viliam: Systém pre ukladanie poznámok v priestore (M. Drozda)

Špilka Marian: Kontextová analýza textu (G. Rozinaj)

Štefanková Zuzana: Prevod zvuku na dynamický obraz (I. Kazlov)

Štefka Pavol: Mobilná aplikácia pre riadenie vzdialených experimentov (K. Žáková)

Šúň Andrej: Tvorba Windows Phone aplikácie na modelovanie a simulovanie Petriho sietí na báze cloudových riešení (C. Cserba)

Táčovská Lenka: Rozpoznávanie chorobných zmien na sietnici (M. Oravec)

Tančibok Ján: Android SysLogger (S. Marček)

Tkáčik Pavol: Automatizovaný sieťový systém efektívneho rozpoznávania originality obrázkov (A. Hambalík)

Tuhý Filip: Návrh a vytvorenie webovej aplikácie na modelovanie a simulovanie Petriho sietí na báze cloudových riešení (C. Cserba)

Uhrecký František: Implementácia kryptografickej knižnice s McEliece kryptosystémom (P. Zajac)

Ustaník Michal: Vzdialené riadenie laboratórneho experimentu (K. Žáková)

Varga Jaroslav: Bigdata Analysis, analýza dát z mobilných zariadení (S. Marček)

Varchola Marek: Vylepšenie autentizačného systému do Android zariadenia (P. Zajac)

Virgovič Miroslav: Metódy klasifikácie prevádzky komunikačných sietí (M. Oravec)

Werdenichová Petra: Cloudove riesenie IaaS (C. Cserba)

Zboroň Matej: Automatizovanie tvorby LPO z časových diagramov (O. Gallo)

XIII.3. ČLENSTVO V ŠTÁTNICOVÝCH KOMISIÁCH

- **Ing. Eugen Antal** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **Ing. Eugen Antal** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **Ing. Štefan Balogh, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS

- **Ing**. **Štefan Balogh, PhD.-** člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **Ing**. **Štefan Balogh, PhD.-** člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **prof. RNDr. Igor Bock, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **Mgr. Csaba Cserba** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **Ing**. **Maroš Čavojský** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **Ing**. **Maroš Čavojský** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **RNDr**. **Viera Čerňanová, PhD.-** člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **RNDr. Karla Čipková, PhD.** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **Dr.rer.nat. Martin Drozda** - predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **Dr.rer.nat. Martin Drozda** - predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **Mgr**. **Tomáš Fabšič** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **Ing**. **Ondrej Gallo, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **Ing**. **Ondrej Gallo, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **Ing**. **Ondrej Gallo, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 8.7.2015 – doména ITvEL
- **Ing**. **Ondrej Gallo, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **prof. RNDr. Otokar Grošek, PhD.** – predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **prof. RNDr. Otokar Grošek, PhD.** – predseda štátnicovej komisie v anglickom jazyku Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **prof. RNDr. Otokar Grošek, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **prof. RNDr. Otokar Grošek, PhD.** – predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **Ing. Alexander Hambalík, PhD.-** člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **Ing. Alexander Hambalík, PhD.-** člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **Ing. Alexander Hambalík, PhD.-** člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **Ing. Viliam Hromada, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **Ing. Viliam Hromada, PhD.** – člen štátnicovej komisie v angllickom jazyku Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS

- **Ing. Viliam Hromada, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **Ing. Viliam Hromada, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména ITvR
- **Mgr. Ing. Matúš Jókay, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.6.2015 – doména MSUS
- **Mgr. Ing. Matúš Jókay, PhD.**- člen štátnicovej komisie v anglickom jazyku Bc. Štúdia pre ŠP AI, FEI STU, 7.6.2015 – doména BIS
- **Mgr. Ing. Matúš Jókay, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **prof. RNDr. Gabriel Juhás, PhD.**- predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **prof. RNDr. Gabriel Juhás, PhD.**- predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **RNDr. Igor Kossaczký, CSc**.- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **RNDr. Igor Kossaczký, CSc**.- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **RNDr. Igor Kossaczký, CSc**.- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **RNDr. Igor Kossaczký, CSc**.- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména ITvR
- **Ing**. **Pavol Marák** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **Ing. Stanislav Marček** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **doc. RNDr. Ľubomír Marko, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. RNDr. Ľubomír Marko, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **doc. RNDr. Ľubomír Marko, PhD.** – člen štátnicovej komisie v anglickom jazyku Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. RNDr. Ľubomír Marko, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **doc. RNDr. Oľga Nánásiová, PhD.** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **doc. RNDr. Oľga Nánásiová, PhD.** - člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **Ing**. **Vladislav Novák** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **Ing**. **Vladislav Novák** - člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **doc. RNDr. Karol Nemoga, PhD.**- predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. RNDr. Karol Nemoga, PhD.**- predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **doc. RNDr. Vladimír Olejček, PhD.**- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS

- **prof. Dr. Ing. Miloš Oravec -** predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **prof. Dr. Ing. Miloš Oravec -** predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **Mgr. Dávid Pancza, PhD.** - člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **RNDr. Elena Pastuchová, PhD.-** člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **doc. Mgr. Marcel Polakovič, PhD.** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. RNDr. Boris Rudolf, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **Ing. Dominik Sopiak** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **Ing. Dominik Sopiak** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **Mgr. Marek Sýs, PhD.-** člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **Mgr. Marek Sýs, PhD.-** člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **Mgr. Zuzana Ševčíková** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **Mgr. Zuzana Ševčíková** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **doc. Ing. Michal Šrámka, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. Ing. Michal Šrámka, PhD.** – člen štátnicovej komisie v anglickom jazyku Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. Ing. Michal Šrámka, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **Ing. Juraj Varga** - člen štátnicovej komisie Bc. štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **Ing. Juraj Varga** - tajomník štátnicovej komisie Ing. štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **doc. Ing. Milan Vojvoda, PhD.** – predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. Ing. Milan Vojvoda, PhD.** – predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS
- **doc. Ing. Milan Vojvoda, PhD.** – predseda štátnicovej komisie v anglickom jazyku Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. Ing. Milan Vojvoda, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **doc. Ing. Milan Vojvoda, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **doc. RNDr. Michal Zajac, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. RNDr. Michal Zajac, PhD.** – člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – doména MSUS

- **doc. RNDr. Michal Zajac, PhD.** – člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **doc. Ing. Pavol Zajac, PhD.**- predseda štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 6.7.2015 – doména BIS
- **doc. Ing. Pavol Zajac, PhD.**- predseda štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 16.6.2015 – doména BIS
- **doc. Ing. Pavol Zajac, PhD.**- člen štátnicovej komisie Ing. Štúdia pre ŠP AI, FEI STU, 17.6.2015 – doména MSUS
- **Mgr.** Michal Zákopčan, PhD.- člen štátnicovej komisie Bc. Štúdia pre ŠP AI, FEI STU, 7.7.2015 – 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 2015

Tatra Mountanains (Volume 64): ***Number Theory and Cryptology '15, editovali*** O. Grošek, K. Nemoga, 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 a učebnice

prof. RNDr. Igor Bock, PhD. – Tatra Mountains Mathematical Publications – 1 recenzia
Mathematical Reviews – 14 prehľadov
Zentralblatt für Mathematik – 17 prehľadov

RNDr. Karla Čipková, PhD. – 1 recenzia pre Journal of Mathematical Cryptology

prof. RNDr. Otokar Grošek, PhD. – 3 recenzie pre Journal of Mathematical Cryptology
- 1 recenzia pre SSHU

doc. Ing. Pavol Zajac, PhD.: TatraMountains Math. Publ., Cryptography and Communications, MathReviews, ZentralBlatt

doc. RNDr. Michal Zajac, PhD.: Math. Slovaca, Acta Math. UK, Bulletin Iranian Math. Soc., Czechoslovak Math. J., Acta UMB Math, MathReviews, ZentralBlatt

XIV.4. Recenzie príspevkov na vedecké konferencie

prof. RNDr. Otokar Grošek, PhD. - Posudok pre CISIS13 Proceedings Jezabel Molina-Gil, Pino Caballero-Gil, Cándido Caballero-Gil and Amparo Fúster-Sabater. Analysis and Implementation of the SNOW 3G Generator Used in 4G/LTE Systems 13.3.2015

doc. RNDr. Michal Zajac, PhD.: 10th Workshop Functional Analysis

XIV.5. Recenzie vedeckých projektov

prof. RNDr. Igor Bock, PhD. – 1 posudok projektu VEGA

doc. RNDr. Michal Zajac, PhD.: VEGA

XV. ORGANIZÁCIA KONFERENCIÍ

NÁZOV KONFERENCIE: 10th Workshop on Functional Analysis and its Applications in Mathematical Physics and Optimal Control
Miesto: Kočovce, Slovenská republika
Dátum: 7.-12.9.2015
Meno: prof. RNDr. Igor Bock, PhD., doc. RNDr. Michal Zajac, PhD., dioc. Mgr. Marcel Polakovič, PhD.
Funkcia: organizácia workshopu

XVI. SEMINÁRE

Seminár: VARIAČNÉ 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.