

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

za rok 2019

riaditeľ ústavu:

Dr. rer. nat. Martin Drozda
e-mail: martin.drozda@stuba.sk

Tel: ++421-2-602 91 109
Fax: ++421-2-654 20 415

I. PRACOVNÍCI

Profesori

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

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. 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.

Odborní asistenti

Ing. Eugen Antal, PhD.
Ing. Štefan Balogh, PhD.
RNDr. Igor Brilla, PhD.
RNDr. Karla Čipková, PhD.
Mgr. Tomáš Fabšič, PhD.
Ing. Ondrej Gallo, PhD.
Ing. Alexander Hambalík, PhD.
Ing. Viliam Hromada, PhD.
Ing. Mgr. Matúš Jókay, PhD.
RNDr. Mária Kečkemétyová, PhD.
Mgr. Jozef Kollár, PhD.
RNDr. Igor Kossaczký, CSc.
Ing. Stanislav Marček, PhD.
RNDr. Ivica Marinová, PhD.
Ing. Vladislav Novák
Mgr. Dávid Pancza, PhD.
RNDr. Elena Pastuchová, PhD.
Mgr. Michal Zákopčan, PhD.

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

Výskumní pracovníci Ing. Maroš Čavojský, PhD.
Ing. Ľuboš Omelina, PhD.
Ing. Dominik Sopiak, PhD.

Interní doktorandi Ing. Zuzana Bukovčíková
Ing. Maroš Čavojský
Ing. Vojtěch Jirka
Ing. Pavol Marák
Ing. Juraj Mažári
Ing. Milan Mladoniczky
Ing. Roderik Ploszek
Ing. Michala Slugeňová
Ing. Dominik Sopiak
Ing. Peter Špaček
Ing. Peter Švec
Ing. Juraj Varga

Externí doktorandi Ing. Vojtěch Jirka
Ing. Igor Kazlov
MUDr. Veronika Kurilová
Ing. Peter Minarovský
Ing. Štefan Počarovský

Externí pracovníci Bc. Tomáš Baka
Ing. Ivana Budinská, PhD.
Bc. Tomáš Gono
Bc. Marián Krkoška
Bc. Katarína Matalíková
Bc. Daniel Neupauer
Bc. Ľubor Pernický
Bc. Simona Šimčíková
Bc. Tomáš Stanko

II. ZARIADENIA

II.1. Výukové a výskumné laboratóriá

- Laboratórium Biometrie a spracovania signálov
- Laboratórium pre Bezpečnosť IT
- Antivírusové laboratórium
- Experimentálne laboratórium ÚIM
- Laboratórium na meranie postranných kanálov
- 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
•Analýza a zložitosť algoritmov (B-AZA)	(5. sem. 2-2 h)	M. Vojvoda
•Databázové systémy (B-DBS)	(4. sem. 2-2 h)	M. Vojvoda/ V. Novák
•Diskrétna matematika (B-DIM)	(4. sem .2-2 h)	M. Polakovič/ J. Kollár
•Diskrétnne udalostné systémy (B-DUS)	(3. sem. 2-2 h)	G.Juhás/ S. Marček/ M. Mladoniczky/
•Klasické šifry (B-KSIF)	(5. sem. 2-2 h)	J. Mažári O.Grošek/ E. Antal
•Lineárna algebra 1 (B-LA1)	(1. sem. 2-2 h)	M. Zajac/ I. Marinová/

●Lineárna algebra 2 (B-LA2)	(2. sem. 2-2 h)	M. Zajac/ E.Pastuchová/ I. Marinová/ O.Nánásiová/ D. Pancza
●Matematická štatistika (B-MASTA)	(3. sem. 2-2 h)	M. Polakovič/ J. Kollár
●Matematika 1 (B-MAT1)	(1. sem. 4-2 h)	M. Zajac/ M.Zákopčan
●Matematika 1 (B-MAT1E)	(1. sem. 4-2 h)	B. Rudolf/ E.Pastuchová/ K. Čipková
●Matematika 1 (B-MAT1I)	(1. sem. 4-2 h)	B. Rudolf
●Matematika 1 op. (B-MAT1I)	(2. sem. 4-2 h)	M. Zajac
●Matematika 1 op. (B-MAT1E)	(2. sem. 4-2 h)	Ľ. Marko/ M.Zákopčan
●Matematika 2 (B-MAT2E)	(2. sem. 2-2 h)	Ľ. Marko/ I. Brilla
●Matematika 2 (B-MAT2)	(2. sem. 2-2 h)	B. Rudolf/ M. Kečkemétyová/ K. Čipková
●Matematika 2 (B-MAT2I)	(2. sem. 2-2 h)	M. Kečkemétyová
●Matematika 2 op. (B-MAT2I)	(3. sem. 2-2 h)	I.Brilla
●Matematika 2 op. (B-MAT2E)	(3. sem. 2-2 h)	I.Brilla
●Matematika 2 op. (B-MAT2)	(3. sem. 2-2 h)	Ľ. Marko/ M. Kečkemétyová
●Matematika 3 (B-MAT3E)	(3. sem. 2-2 h)	Ľ. Marko/ O. Nánásiová
●Matematika 3 (B-MAT3)	(3. sem. 2-2 h)	Ľ. Marko/ O. Nánásiová
●Matematika 4 (B-MAT4)	(3. sem. 2-2 h)	Ľ. Marko/ O.Nánásiová
●Objektovo orientované programovanie (B-OOP)	(3. sem. 2-2 h)	G. Juhás/ O. Gallo/ J. Mažári/ M. Mladoniczky
●Operačné systémy (B-OS)	(5. sem. 2-2 h)	M. Šrámka/ M. Jókay/ R. Ploszek/ P. Švec
●Počítačová kriminalita (B-PKRIM)	(6. sem. 2-2 h)	K. Nemoga/ Š. Balogh/ R. Ploszek
●Počítačové siete (B-PS)	(3. sem. 2-2 h)	M.Oravec/ D. Sopiak/ Z. Bukovčíková/ A. Hambalík
●Programovacie techniky (B-PT)	(3. sem. 3-2 h)	M. Drozda/ P. Marák/ V. Novák
●Programovanie 1 (B-PROG1)	(1. sem. 2-2 h)	P. Zajac/ T. Fabšič/

●Programovanie 2 (B-PROG2)	(2. sem. 2-2 h)	V. Hromada/ P. Zajac/ P. Marák/ S. Marček/ P. Špaček
●Rýchle algoritmy (B-RAL)	(6. sem. 2-2 h)	K. Nemoga/ K. Čipková
●Softvérové inžinierstvo (B-SWI)	(5. sem. 2-2 h)	M. Šrámka/ O. Gallo
●Teoretické základy informatiky (B-TZI)	(4. sem. 2-2 h)	O. Grošek
●Vývoj softvérových aplikácií (B-VSA)	(6. sem. 2-2 h)	G. Juhás/ I. Kossaczský/ E. Antal
●Základy finančnictva (B-ZFI)	(4. sem. 2-2 h)	M. Zákopčan

III.2. Inžinierske štúdium (Ing.)

●Algoritmy a dátové štruktúry (I-ADS)	(4. sem. 2-2 h)	M. Vojvoda/ T. Fabšič/ A. Hambalík
●Architektúra softvérových systémov (I-ASOS)	(3. sem. 2-2 h)	G. Juhás/ I. Kossaczský/ E. Antal
●Automaty a formálne jazyky (I-AFJ)	(2. sem. 2-2 h)	O. Grošek/ V. Hromada
●Bezpečnosť informačných systémov s pohľadu praxe (I-BISPP)	(2. sem. 3-2 h)	M. Šrámka/ Š. Balogh
●Biometria (I-BIOM)	(3. sem. 2-2 h)	M. Oravec/ D. Sopiak/ Z. Bukovčiková
●Kódovanie (KOD_I) - FIIT	(1. sem. 2-2 h)	K. Čipková
●Logika (I-LOG)	(1.+3. sem. 2-2 h)	K. Nemoga/ K. Čipková
●Matematika (I-MAT)	(1. sem. 2-2 h)	B. Rudolf
●Mobilné výpočty (I-MOBV)	(3. sem. 2-2 h)	M. Drozda/ M. Čavojský
●Modelovanie a simulácia udalostných systémov (I-MSUS)	(1. sem. 2-2 h)	G. Juhás/ M. Mladoniczky/ J. Mažári
●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
●Počítačové siete 2 (I-PS2)	(2.sem. 2-2 h)	M. Drozda/ S. Marček
●Reprezentácia a získavanie znalostí (I-RZZ),	(2. sem. 2-2 h)	K. Nemoga / I. Kossaczský/ I. Budinská/

• Spoločenské, morálne a právne súvislosti vývoja informačných systémov (I-SMPSVIS)	(3. sem. 3-0 h)	Š. Balogh
• Strojové učenie a neurónové siete (I-SUNS)	(1. sem. 2-2 h)	M. Šrámka M. Oravec/ D. Sopiak/ Z. Bukovčíková
• Šifrovanie v komunikačných sieťach (I-SKS)	(1. sem. 3-2 h)	K. Nemoga/ T. Fabšič
• Úvod do počítačovej bezpečnosti (I-UPB)	(1. sem. 2-1 h)	P. Zajac/ Š. Balogh/ P. Špaček/ P. Švec
• Základy kryptografie (I-ZKRY)	(1. sem. 2-2 h)	O. Grošek

III.3. Doktorandské štúdium (PhD.)

- Dizertačná skúška D-DS-AI
- Dizertačný projekt I D-DP1-AI
- Dizertačný projekt II D-DP2-AI
- Dizertačný projekt III D-DP3-AI
- Dizertačný projekt IV D-DP4-AI
- Odborná angličtina D-AJ
- Predmet špecializácie Aplikovaná informatika I D-PS1-AI
- Predmet špecializácie Aplikovaná informatika II D-PS2-AI
- Teória odboru Aplikovaná informatika D-T-AI
- Vedecká práca I D-VP1-AI
- Vedecká práca II D-VP2-AI
- Vedecká práca III D-VP3-AI
- Vedecká práca IV D-VP4-AI

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

• Algoritmy a dátové štruktúry	M. Vojvoda
• Bakalársky projekt	O. Gallo
• Diskrétna matematika	M. Polakovič
• Mobilné výpočty	M. Drozda
• Modelovanie a simulácia udalostných systémov	G. Juhás
• Operačné systémy	M. Jókay/ R. Ploszek
• Základy kryptografie	O. Grošek

IV. VÝSKUMNÉ PROJEKTY

IV.1. Projekty VEGA, ESF, APVV a iné riešené v roku 2019 na ÚIM

Číslo projektu: VEGA 1/0159/17

Názov projektu: Bezpečná postkvantová kryptografia

Zodpovedný riešiteľ: prof. Ing. Pavol Zajac, PhD.

Zástupca vedúceho projektu: Ing. Viliam Hromada, PhD.

Spoluriešitelia z ÚIM v roku 2019: prof. RNDr. Otokar Grošek, PhD., doc. Ing. Milan Vojvoda, PhD., Mgr. Ing. Matúš Jókay, PhD., Ing. Alexander Hambalík, PhD., Ing. Eugen Antal, PhD., Ing. Ondrej Gallo, PhD., Ing. Štefan Balogh, PhD., Mgr. Tomáš Fabšič, PhD., Ing. Michala Slugeňová, Ing. Peter Špaček, doc. RNDr. Oľga Nánásiová, PhD., RNDr. Karla Čipková, PhD., Mgr. Jozef Kollár, PhD.

Doba riešenia: 2017– 2020

Číslo projektu: VEGA 1/0867/17

Názov projektu: MLbiomedia- Pokročilé metódy strojového učenia na návrh biometrických a medicínskych systémov

Zodpovedný riešiteľ: prof. Dr. Ing. Miloš Oravec

Spoluriešitelia z ÚIM v roku 2019: Ing. Dominik Sopiak, PhD., Ing. Zuzana Bukovčiková, Ing. Vojtěch Jirka, Ing. Luboš Omelina, PhD., MUDr. Veronika Kurilová

Doba riešenia: 2017 - 2020

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

IV.3.1. Multilaterálna spolupráca

Názov projektu: Secure Communication in the Quantum Era

Číslo projektu: NATO SPS Project G5448

Zahraniční partneri: University of Malta, Malta,
Universidad Rey Juan Carlos, Španielsko
Florida Atlantic University, USA

Vedúci projektu za krajiny z NATO: prof. RNDr. Otokar Grošek, PhD.

Vedúci projektu za partnerskú krajinu: Dr. Christian Colombo (University of Malta)

Spoluvedúci projektu: Dr. Maria-Isabel Gonzales Vasco (Universidad Rey Juan Carlos, Madrid)
Prof. Rainer Steinwandt (Florida Atlantic University)

Riešitelia z ÚIM v roku 2019: doc. RNDr. Karol Nemoga, PhD., prof. Ing. Pavol Zajac, PhD., Ing. Viliam Hromada, PhD., Mgr. Tomáš Fabšič PhD., Ing. Ondrej Gallo PhD., Ing. Peter Špaček

Riešitelia z University of Malta: Gordon Pace

Riešitelia z Universidad Rey Juan Carlos: Manuel Arrayás, Angel L. Pérez del Pozo, Jose Luis Trueba

Riešitelia z Florida Atlantic University: Shi Bai, Shaun Miller, Edoardo Persichetti

Trvanie projektu: 2018-2021

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

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 2019: RNDr. Igor Brilla, PhD.

Doba riešenia: 01.07.2016-31.12.2019

Názov projektu: Inteligentné mechatronické systémy

Vedúci projektu: prof. Ing. Alena Kozáková, PhD., ÚAMt FEI STU

Spoluriešitelia z ÚIM v roku 2019: prof. RNDr. Igor Bock, PhD., doc. RNDr. Michal Zajac, PhD., RNDr. Mária Kečkemetyová, PhD.

Doba riešenia: 01.01.2017-31.12.2019

Číslo projektu: ITMS 312011G208 MŠVVaŠ SR

Názov projektu: Informatika ako nástroj rozvoja znalostnej ekonomiky

Vedúci projektu: Ing. Fedor Lehocki, PhD., MPH, Národné centrum telemedicínskych služieb

Spoluriešiteľ z ÚIM v roku 2019: Ing. Alexander Hambalík, PhD., doc. RNDr. Karol Nemoga, CSc., Ing. Vladislav Novák, Ing. Roderik Ploszek, Ing. Peter Špaček

Doba riešenia: 01.11.2018-30.09.2020

Číslo projektu: ITMS 312011F318 MŠVVaŠ SR

Názov projektu: Med&Com - osvojenie si nových spôsobov elektronickej komunikácie pacient-lekár a lekár-pacient

Vedúci projektu: MUDr. Marian Zelina, Sanitas Slovaca - agentúra pre rozvoj zdravia na Slovensku, o.z.

Spoluriešiteľ z ÚIM v roku 2019: Alexander Hambalík, Ing., PhD.

Doba riešenia: 01.11.2018-30.09.2020

Číslo projektu: VEGA grant 1/0039/17

Názov projektu: Real-world problem solving by means of complex networks

Vedúci projektu: prof. Beňušková FMFI UK

Spoluriešiteľ z ÚIM v roku 2019: doc. RNDr. Boris Rudolf, PhD.

Doba riešenia: 2017-2019

V. SPOLUPRÁČA

V.1. Domáca spolupráca

V.1.1. Pozvané prednášky

Meno: Mgr. Tomáš Fabšič, PhD.

Miesto: Satori Stage, Mickiewiczova 2246/9, 811 07 Bratislava

Prednáška: Šifrovanie a kvantové počítače
(prednáška bola súčasťou prednáškového cyklu Vedatour)

Dátum: 30.9.2019

Meno: prof. RNDr. Otokar Grošek, PhD.

Miesto: B-Klub FEI STU

Prednáška: Existuje dokonalá náhodnosť?

Dátum: 9.10.2019

V.1.2. Spolupráca s domácimi inštitúciami

- Nadácia VÚB
- Slovenská sporiteľňa
- Kriminálny 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 (doc. RNDr. Mária Bohdalová, PhD.)
- ÚIAa FCHPT STU (prof. RNDr. Anna Kolesárová, CSc.)
- Katedra matematiky a deskriptívnej geometrie SvF STU (prof. RNDr. Radko Mesiar, PhD., prof. RNDr. Jozef Širáň, DrSc., prof. RNDr. Magdaléna Komorníková, PhD., prof. RNDr. Karol Mikula, DrSc., prof. RNDr. Martin Kalina, PhD., doc. Mgr. Gejza Jenča, PhD., RNDr. Ľubica Valášková, PhD.)
- Katedra matematickej analýzy FMFI UK (doc., RNDr., Zbyněk Kubáček, CSc.)
- Katedra matematiky SjF STU (doc. RNDr. Daniela Velichová, CSc., Mgr. Monika Kováčová, PhD.)
- IBM Slovensko, s.r.o.
- Ministerstvo obrany SR
- Sanitas Slovaca - agentúra pre rozvoj zdravia na Slovensku, o.z.

- Katedra informatiky AOS Liptovský Mikuláš (doc. RNDr. Ferdinand Chovanec, CSc., RNDr. Eva Drobná, PhD.)

V.1.3. Pozvané prednášky domácich odborníkov

V.2. Zahraničná spolupráca

V.2.1. Pozvané prednášky

V.2.1.1. Zahraniční hostia

Host' (adresa): prof. Jaroslaw Pykacz, Gdanská univerzita, Poľsko

Termín: 15.5.2019

Prednáška: Berge equilibrium – the forgotten notion of game theory

V.2.1.2. Pracovníci ÚIM v zahraničí

Meno: Ing. Viliam Hromada, PhD.

Miesto: CYBERSEC Conference, Katowice, Poľsko

Prednáška: Acoustic Side-Channels in Cryptography

Dátum: 30.10.2019

Meno: Ing. Eugen Antal, PhD., prof. RNDr. Otokar Grošek, PhD.,

Miesto: Mikulášska kryptobesídka 2019, Praha, Česká republika

Prednáška: Cipher used during the Slovak State

Dátum: 6.12.2019

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)
- University of Ljubljana, Ljubljana, Slovenia (izr. prof. dr. Janko Bračič).
- Institut de Mathematiques, Université Louis Pasteur, France
- Eszterházy Károly Egyetem, Eger, Maďarsko (Dr. Kis Tóth Lajos, Tóthné dr. Parázsó Lenke)
- Matematický ústav AVČR (doc. RNDr. Vladimír Müller, 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 Gdansk, Poland (prof. Jaroslaw Pykacz)

- University of Houston, Department of Biomedical Engineering, USA (prof. Metin Akay)
- University of Malta, Malta (Dr. Christian Colombo)
- Universidad Rey Juan Carlos, Madrid, Spain (Dr. María Isabel González Vasco)

V.2.3. Zahraniční hostia

V.2.4. Pobyty pracovníkov ÚIM v zahraničí

Meno: Ing. Peter Špaček

Miesto: Maltská univerzita, Msida, Malta

Účel: štúdijná stáž

Dátum: 23.9.2019-4.2.2020

V.2.5. Zahraničné cesty

Meno: prof. Ing. Pavol Zajac, PhD.

Miesto: Maltská univerzita, Malta

Zámer cesty: rokovanie s partnermi a práca na spoločnom projekte s C. Palestini a D. Beten

Dátum: 31.3.-4.4.2019

Meno: prof. RNDr. Otokar Grošek, PhD.

Miesto: Maltská univerzita, Malta

Zámer cesty: rokovanie s partnermi a práca na spoločnom projekte s C. Palestini a D. Beten

Dátum: 31.3.-4.4.2019

Meno: Mgr. Tomáš Fabšič, PhD.

Miesto: Madrid, Španielsko, Universidad Rey Juan Carlos

Zámer cesty: pracovné stretnutie projektu Nato G 5448

Dátum: 23.-27.9.2019

Meno: Ing. Peter Špaček

Miesto: Madrid, Španielsko, Universidad Rey Juan Carlos

Zámer cesty: pracovné stretnutie projektu Nato G 5448

Dátum: 23.-27.9.2019

Meno: prof. RNDr. Otokar Grošek, PhD.

Miesto: Madrid, Španielsko, Universidad Rey Juan Carlos

Zámer cesty: pracovné stretnutie projektu Nato G 5448

Dátum: 23.-27.9.2019

Meno: prof. Ing. Pavol Zajac, PhD.

Miesto: Madrid, Španielsko, Universidad Rey Juan Carlos

Zámer cesty: pracovné stretnutie projektu Nato G 5448

Dátum: 23.-27.9.2019

V.2.6. Stáže zahraničných pracovníkov na ÚIM FEI STU

Host' (adresa): prof. Jaroslaw Pykacz, Gdanská univerzita, Poľsko

Termín: 1.4-31.5.2019

Účel: spolupráca na vedeckom článku s doc. O. Nánásiovou

V.3. Členstvo v medzinárodných organizáciách a spoločnostiach¹

- **prof. RNDr. Igor Bock, PhD.** je členom GAMM
- **RNDr. Igor Brilla, PhD.** je členom ISIMM a IACM.
- **Dr.rer.nat. Martin Drozda** je členom ACM.
- **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.
- **doc. RNDr. Oľga Nánásiová, CSc.,** členka ENS v Nemecku, členka IQSA.
- **doc. RNDr. Karol Nemoga, PhD.** je členom IACR a SIAM.
- **prof. Dr. Ing. Miloš Oravec** je členom IEEE IET.
- **RNDr. Elena Pastuchová, PhD.** je členkou ENS v Nemecku.

VI. INÉ AKTIVITY

VI.1. Akademické a iné funkcie

- **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 SvF 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.
- **Dr.rer.nat. Martin Drozda** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na STU
- **Dr.rer.nat. Martin Drozda** je členom riadiaceho grémia medzinárodnej spolupráce Akcia Rakúsko-Slovensko, spolupráca vo vede a vzdelávaní.
- **prof. RNDr. Otokar Grošek, PhD.** bol členom Vedeckej rady FEI STU do mája 2019.
- **prof. RNDr. Otokar Grošek, PhD.** bol predsedom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na STU do mája 2019.

¹ AMS - American Mathematical Society

ACM - Association for Computing Machinery

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

- **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. Oľga Nánásiová, PhD.** je členka Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU
- **doc. RNDr. Oľga Nánásiová, PhD.** je členka Odborovej komisie (OK) doktorandského štúdia v odbore 9-1-11 Pravdepodobnosť a matematická štatistika na UMB v Banskej Bystrici od r. 2009.
- **doc. RNDr. Oľga Nánásiová, PhD.** je členka komisie pre štátne skúšky doktorandského štúdia (dizertačná skúška, obhajoba dizertačnej práce) v študijných programoch 3.3.15. manažment a 3.3.22. podnikový manažment **na FM UK**
- **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
- **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 člen komisie KEGA (Kultúrna a edukačná grantová agentúra Ministerstva školstva, vedy, výskumu a športu SR)
- **prof. Dr. Ing. Miloš Oravec** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na STU
- **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. Ing. Michal Šrámka, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na STU
- **doc. Milan Vojvoda, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na 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
- **doc. RNDr. Michal Zajac, PhD.** je členom AS FEI STU

VI.2. Členstvo v domácich spoločnostiach a organizáciách²

- **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. Olga Nánásiová, CSc.** je členkou celoštátneho výboru SSM, členkou JSMF a Slovenskej štatistickej a demografickej spoločnosti
- **doc. RNDr. Karol Nemoga, PhD.** je členom JSMF a Slovenského plynárenského a naftového zväzu
- **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

VI.3. Vedenie prác študentov v sút'aziach

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

VII. PUBLIKÁCIE

ADC Vedecké práce v zahraničných karentovaných časopisoch

ADC01 GROŠEK, Otokar - ANTAL, Eugen - FABŠIČ, Tomáš. Remarks on breaking the Vigenere autokey cipher. In *Cryptologia*. Vol. 43, Iss. 6 (2019), s. 486-496. ISSN 0161-1194 (2018: 0.417 - IF, Q3 - JCR Best Q, 0.109 - SJR, Q4 - SJR Best Q). V databáze: CC: 000469567400001 ; DOI: 10.1080/01611194.2019.1596997.

ADC02 ZAJAC, Pavol. Hybrid encryption from McEliece cryptosystem with pseudo-random error vector. In *Fundamenta Informaticae : 17th Central European Conference on Cryptology. Warsaw, Poland. July 4-6, 2017*. Vol. 169, (2019), s. 345-360. ISSN 0169-2968 (2018: 1.204 - IF, Q2 - JCR Best Q, 0.355 - SJR, Q2 - SJR Best Q). V databáze: CC: 000489902500006 ; SCOPUS: 2-s2.0-85073715984 ; DOI: 10.3233/FI-2019-1851.

ADF Vedecké práce v ostatných domácich časopisoch

ADF01 BRILLA, Igor - JANÍČEK, František. Numerical determination of voltage potential inside nonhomogeneous media using variational methods. In *Acta Electrotechnica et Informatica*. Vol. 19, No. 1 (2019), s. 25-31. ISSN 1335-8243.

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

ADM01 NÁNÁSIOVÁ, Oľga - VALÁŠKOVÁ, Ľubica - ČERŇANOVÁ, Viera. Probability measures and logical connectives on quantum logics. In *Journal of Automation, Mobile Robotics & Intelligent Systems*. Vol. 13, No. 3 (2019), s. 64-73. ISSN 1897-8649 (2018: 0.134 - SJR, Q4 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85078881819 ; DOI: 10.14313/JAMRIS/3-2019/29.

ADM02 ZAJAC, Pavol - ŠPAČEK, Peter. A new type of signature scheme derived from a MRHS representation of a symmetric cipher. In *Infocommunications journal*. Vol. 11, No. 4 (2019), s. 23-30. ISSN 2061-2079 (2018: 0.129 - SJR, Q4 - SJR Best Q).

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

ADN01 ANTAL, Eugen - JAVORKA, Peter - HLIBOKÝ, Tomáš. Cryptanalysis of the columnar transposition using meta-heuristics. In *Tatra Mountains Mathematical Publications : Number theory, algebra and cryptology '18*. Vol. 73, (2019), s. 39-60. ISSN 1210-3195 (2018: 0.226 - SJR, Q3 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85072302081.

ADN02 ZAJAC, Pavol - ŠPAČEK, Peter. Preventing potential backdoors in bike algorithm. In *Tatra Mountains Mathematical Publications : Number theory, algebra and cryptology '18*. Vol. 73, (2019), s. 179-193. ISSN 1210-3195 (2018: 0.226 - SJR, Q3 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85072285502 ; DOI: 10.2478/tmmp-2019-0013.

AFC Publikované príspevky na zahraničných vedeckých konferenciách

AFC01 ANTAL, Eugen - ZAJAC, Pavol - GROŠEK, Otokar. Cryptology in the Slovak state during WWII. In *HistoCrypt 2019 : 2nd International conference on historical*

cryptology. Mons, Belgium. June 23-26, 2019. Linköping : University Electronic Press, 2019, S. 23-30. ISBN 978-91-7685-087-9.

- AFC02 BALOGH, Štefan - MOJŽIŠ, Ján. New direction for malware detection using system features. In *IDAACS 2019 : 10th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Vol. 2. Metz, France. September 18-21, 2019.* Danvers : IEEE, 2019, S. 176-183. ISBN 978-1-7281-4068-1. V databáze: IEEE: 8924358 ; SCOPUS: 2-s2.0-85077060167.
- AFC03 BOCK, Igor - KEČKEMÉTYOVÁ, Mária. An optimal design of an elastic plate in a dynamic contact with a rigid obstacle. In *PAMM. Proceedings of Applied Mathematics and Mechanics : 90th Annual Meeting of the International Association of Applied Mathematics and Mechanics (GAMM). Wien, Austria. February 18-22, 2019.* Vol. 19, Iss. 1 (2019), Art. no. 201900183 [2] s. ISSN 1617-7061. V databáze: DOI: 10.1002/pamm.201900183.
- AFC04 BRILLA, Igor - JANIČEK, František. Numerical determination of voltage potential inside nonhomogeneous media using variational approach. In *CAIP'2019 : 14^o Congreso interamericano de computación aplicado a la industria de procesos. Lima, Perú. 21 al 24 de Octubre del 2019.* Lima : Pontificia Universidad Católica del Perú, 2019, S. 857-867. ISBN 978-612-48025-3-9.
- AFC05 ČAVOJSKÝ, Maroš - DROZDA, Martin. Comparison of user trajectories with the Needleman-Wunsch algorithm. In *Mobile Computing, Applications, and Services : 10th EAI International conference, MobiCASE 2019. Hangzhou, China. June 14-15, 2019.* Cham : Springer, 2019, S. 141-154. ISBN 978-3-030-28467-1. V databáze: DOI: 10.1007/978-3-030-28468-8_11 ; SCOPUS: 2-s2.0-85075721719.
- AFC06 HAMBALÍK, Alexander - MARÁK, Pavol. Príprava študentov, odborníkov pre oblasť biometrie. In *Trendy ve vzdělávání.* Roč. 12, č. 2 (2019), s. 28-37. ISSN 1805-8949. V databáze: DOI: 10.5507/tvv.2019.010.
- AFC07 VIZVÁRY, Ladislav - SOPIAK, Dominik - ORAVEC, Miloš - BUKOVČIKOVÁ, Zuzana. Image quality detection using the siamese convolutional neural network. In *Proceedings ELMAR-2019 : 61st International symposium. Zadar, Croatia. September 23-25, 2019.* 1. ed. Zagreb : University of Zagreb, 2019, S. 109-112. ISSN 1334-2630. ISBN 978-1-7281-2182-6. V databáze: IEEE: 8918678 ; SCOPUS: 2-s2.0-85077541837.

AFD Publikované príspevky na domácich vedeckých konferenciách

- AFD01 BUKOVČIKOVÁ, Zuzana - ORAVEC, Miloš. Gender classification based on descriptors from deep facial recognition model. In *ELITECH'19 [elektronický zdroj] : 21st Conference of doctoral students. Bratislava, Slovakia. May 29, 2019.* 1. ed. Bratislava : Vydavateľstvo Spektrum STU, 2019, CD-ROM, [5] s. ISBN 978-80-227-4915-2.
- AFD02 HAMBALÍK, Alexander. Ciele kyberútokov sa rozširujú na menej chránené zariadenia sietí. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek) : Vedecká konferencia s medzinárodnou účasťou. Bratislava,*

Slovensko. 4.6.2019. Bratislava : Akadémia Policajného zboru v Bratislave, 2019, S. 11-20. ISBN 978-80-8054-820-9.

- AFD03 JUHÁSOVÁ, Ana - JUHÁS, Gabriel - MOLNÁR, Ľudovít - ONDRIŠOVÁ, Miriam - MAŽÁRI, Juraj - MLADONICZKY, Milan. IT induced innovations: Digital transformation and process automation. In *ICETA 2019 : 17th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning. Starý Smokovec, Slovakia. November 21-22, 2019.* Danvers : IEEE, 2019, S. 322-329. ISBN 978-1-7281-4967-7.
- AFD04 ONDRIŠOVÁ, Miriam - MOLNÁR, Ľudovít - JUHÁS, Gabriel - JUHÁSOVÁ, Ana - MAŽÁRI, Juraj - MLADONICZKY, Milan. Story of artificial intelligence: research and publications behind. In *ICETA 2019 : 17th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning. Starý Smokovec, Slovakia. November 21-22, 2019.* Danvers : IEEE, 2019, S. 581-586. ISBN 978-1-7281-4967-7.
- AFD05 PLOSZEK, Roderik. Upgrading complex single-threaded application to support concurrency. In *ELITECH'19 [elektronický zdroj] : 21st Conference of doctoral students. Bratislava, Slovakia. May 29, 2019.* 1. ed. Bratislava : Vydavateľstvo Spektrum STU, 2019, CD-ROM, [8] s. ISBN 978-80-227-4915-2.

BCI Skriptá a učebné texty

- BCI01 DROZDA, Martin. *Zbierka príkladov v jazyku C++* [elektronický zdroj]. 1. vyd. Bratislava : Vydavateľstve SPEKTRUM STU, 2019. CD-ROM, 96 s. ISBN 978-80-227-4968-8.

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

- BDM01 MATYÁŠ, Václav - ZAJAC, Pavol - HAJNÝ, Jan - SÝS, Marek. Special issue on cryptology - Guest editorial. In *Infocommunications journal*. Vol. 11, No. 4 (2019), s. 1. ISSN 2061-2079 (2018: 0.129 - SJR, Q4 - SJR Best Q).

BEE Odborné práce v zahraničných zborníkoch (konferenčných aj nekonferenčných)

- BEE01 ANTAL, Eugen - SOJÁK, Peter. Solving historical ciphers using evolutionary programming. In *Central European Conference on Cryptology 2019 : Telč, Czech Republic. June 12-14, 2019.* Brno : Masaryk University, 2019, S. 65-66.
- BEE02 FIRČA, Michal - ANTAL, Eugen. Porovnanie metód identifikácie samohlások v texte a ich využitie pri lúštení klasických šifier. In *Mikulášská kryptobesídka 2019 : sborník příspěvků. Praha, Česká republika. 5.-6.12.2019.* 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2019, S. 35-36.
- BEE03 MACHOVEC, Jakub - ANTAL, Eugen. Lúštenie šifrovanej korešpondencie Marie Antoinette. In *Mikulášská kryptobesídka 2019 : sborník příspěvků. Praha, Česká republika. 5.-6.12.2019.* 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2019, S. 31-32.
- BEE04 PERNICKÝ, Ľubor - ZAJAC, Pavol. Integrácia postkvantovej kryptografie do Android aplikácie. In *Mikulášská kryptobesídka 2019 : sborník příspěvků. Praha,*

Česká republika. 5.-6.12.2019. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2019, S. 37-38.

- BEE05 ŠPAČEK, Peter. Quantum resistant handshake: code-based KEM candidates. In *Central European Conference on Cryptology 2019 : Telč, Czech Republic. June 12-14, 2019*. Brno : Masaryk University, 2019, S. 37-38.
- BEE06 ŠVEC, Peter - JÓKAY, Matúš. Video steganography based on synchronization timestamps. In *Mikulášská kryptobesídka 2019 : sborník příspěvků. Praha, Česká republika. 5.-6.12.2019*. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2019, S. 33-34.
- BEE07 ZAJAC, Pavol. Code-based signature scheme derived from a MRHS representation of an AES encryption. In *Central European Conference on Cryptology 2019 : Telč, Czech Republic. June 12-14, 2019*. Brno : Masaryk University, 2019, S. 39-42.

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

- BFA01 ANTAL, Eugen - GROŠEK, Otokar. O šifrách, ktoré sa používali počas "Slovenského štátu". In *Mikulášská kryptobesídka 2019 : sborník příspěvků. Praha, Česká republika. 5.-6.12.2019*. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2019, S. 29.
- BFA02 JÓKAY, Matúš - ŠPAČEK, Peter - ZAJAC, Pavol. Linear and differential properties of S-boxes with respect to modular addition. In *BFA 2019 : The 4th international workshop on boolean functions and their applications. Florencia, Italy. June 16-21, 2019*. Bergen : University of Bergen, 2019, S. 13.
- BFA03 JUHÁS, Gabriel - MAŽÁRI, Juraj - MLADONICZKY, Milan - JUHÁSOVÁ, Ana. Implementation semantics of Petriflow models. In *Algorithms and Tools for Petri nets : Proceedings of the Workshop AWPN 2019. Hagen, German. October 10-11, 2019*. Hagen : FernUniversität in Hagen, 2019, S. 45-46.
- BFA04 MAŽÁRI, Juraj - JUHÁS, Gabriel - MLADONICZKY, Milan. Execution of event chains in a Petriflow model. In *Algorithms and Tools for Petri nets : Proceedings of the Workshop AWPN 2019. Hagen, German. October 10-11, 2019*. Hagen : FernUniversität in Hagen, 2019, S. 30-31.
- BFA05 MLADONICZKY, Milan - JUHÁS, Gabriel - MAŽÁRI, Juraj. Cluster inter-process communication in Petriflow language. In *Algorithms and Tools for Petri nets : Proceedings of the Workshop AWPN 2019. Hagen, German. October 10-11, 2019*. Hagen : FernUniversität in Hagen, 2019, S. 10-11.
- BFA06 ŠPAČEK, Peter - COLOMBO, Christian - VELLA, Mark. Using TEE and RV in PQ-TLS communication. In *CSAW '19 : Computer science annual workshop. Msida, Malta. November 6-8, 2019*. Msida : University of Malta, 2019, S. 14.

DAI Dizertačné a habilitačné práce

- DAI01 ČAVOJSKÝ, Maroš. *Metodológia zaznamenávania pohybu používateľa : dátum obhajoby 1.7.2019, č. ved. odboru 9-2-9*. Bratislava :. STU v Bratislave FEI, 2019.

128 s. Dostupné na internete:
<http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=130769>.

- DAI02 KAZLOV, Igor. *Analýza udalostných systémov s viacerými inštanciami : dátum obhajoby 26.8.2019, č. ved. odboru 9-2-9*. Bratislava :. STU v Bratislave FEI, 2019. 72 s., CD-ROM. Dostupné na internete:
<http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=114835>.

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

- FAI01 ANTAL, Eugen (ed.) - SCHMEH, Klaus (ed.). *HistoCrypt 2019 : 2nd International conference on historical cryptology. Mons, Belgium. June 23-26, 2019*. Linköping : University Electronic Press, 2019. 132 s. Linköping Electronic Conference Proceedings No. 158. ISBN 978-91-7685-087-9.
- FAI02 GROŠEK, Otokar (ed.) - NEMOGA, Karol (ed.) - PAŠTĚKA, Milan (ed.) - ZAJAC, Pavol (ed.). *Tatra Mountains Mathematical Publications : Number theory, algebra and cryptology '18*. Bratislava : Slovak Academy of Sciences, 2019. 193 s. Dostupné na internete: <<https://www.mat.savba.sk/ojs/index.php/TATRA/issue/view/37>>. ISSN 1210-3195.

Štatistika: kategória publikačnej činnosti

ADC	Vedecké práce v zahraničných karentovaných časopisoch	2
ADF	Vedecké práce v ostatných domácich časopisoch	1
ADM	Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS	2
ADN	Vedecké práce v domácich časopisoch registrovaných v databázach Web of Science alebo SCOPUS	2
AFC	Publikované príspevky na zahraničných vedeckých konferenciách	7
AFD	Publikované príspevky na domácich vedeckých konferenciách	5
BCI	Skriptá a učebné texty	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)	7
BFA	Abstrakty odborných prác zo zahraničných podujatí (konferencie...)	6
DAI	Dizertačné a habilitačné práce	2
FAI	Redakčné a zostavovateľské práce knižného charakteru (bibliografie, encyklopédie, katalógy, slovníky, zborníky...)	2
Súčet		38

VIII. VÝCHOVA VEDECKÝCH PRACOVNÍKOV

VIII.1. Interní doktorandi

Doktorand: Ing. Zuzana Bukovčiková

Školiteľ: prof. Dr. Ing. Miloš Oravec

Forma vzdelávania: doktorandské štúdium – interná forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM, FEI STU

Dizertačná skúška: 15.3.2019

Predpokladaný termín ukončenia:

Téma práce: Obsahovo orientované prehl'adávanie obrazov pre biometriu

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: 2018

Téma práce: Metodológia a systém na efektívne testovanie mobilných aplikácií

Obhajoba: 1.7.2019

Doktorand: Ing. Michala Slugeňová, rod. Gulášová

Školiteľ: doc. Ing. Milan Vojvoda, PhD.

Školiteľ špecialista: Ing. Matúš Jókay, PhD.

Forma vzdelávania: doktorandské štúdium – interná forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM, FEI STU

Dizertačná skúška: 2.3.2018

Predpokladaný termín ukončenia:

Téma práce: Steganografia a stegoanalýza

Prerušené: 01. 12. 2018 - 01. 12. 2021

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: 9/2020

Téma práce: Charakteristické vlastnosti odtlačkov prstov a dlaní a ich automatické rozpoznávanie

Prerušené: 17. 09. 2019 - 02. 09. 2020

Doktorand: Ing. Juraj Mažári

Školiteľ: prof. Ing. Gabriel Juhás, PhD.

Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 3.6.2019
Téma práce: Syntéza workflow procesov z pozorovaného správania

Doktorand: Ing. Milan Mladoniczky
Školiteľ: prof. Ing. Gabriel Juhás, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 3.6.2019
Téma práce: Analýza a korekcia workflow procesov so zdieľanými zdrojmi

Doktorand: Ing. Roderik Ploszek
Školiteľ: doc. Ing. Milan Vojvoda, PhD.
Školiteľ špecialista: Ing. Matúš Jókay, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Téma práce: Bezpečnosť operačných systémov

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: 2019
Téma práce: Návrh multimodálneho biometrického systému
Prerušenie: 1.9.2017 -2.9.2019
Obhajoba: 17.1.2019

Doktorand: Ing. Peter Špaček
Školiteľ: prof. Ing. Pavol Zajac, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 7.5.2019
Predpokladaný termín ukončenia:
Téma práce: Bezpečná postkvantová kryptografia

Doktorand: Ing. Peter Švec
Školiteľ: prof. Ing. Pavol Zajac, PhD.
Školiteľ špecialista: Ing. Štefan Balogh, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU

Dizertačná skúška:

Predpokladaný termín ukončenia:

Téma práce: Ontologická reprezentácia pre bezpečnosť informačných systémov

Doktorand: Ing. Juraj Varga

Školiteľ: prof. 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

Prerušenie: 01.8.2016 - 31.7.2018

Obhajoba: 18.1.2019

VIII.2. Externí doktorandi

Doktorand: Ing. Vojtěch Jirka

Školiteľ: prof. Dr. Ing. Miloš Oravec

Forma vzdelávania: doktorandské štúdium – externá forma, do 1.9.2018 interná forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM, FEI STU

Dizertačná skúška: 22.5.2014

Predpokladaný termín ukončenia: 2018

Téma práce: Nové metódy biometrického rozpoznávania tváří v neriadených podmienkach využitím metód strojového učenia

Prerušenie: 1.7.2015-2.7.2018

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

Prerušenie: 31.8.2017 - 30.8.2018

Obhajoba: 26.8.2019

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. 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: Ing. Štefan Počarovský

Školiteľ: prof. RNDr. Gabriel Juhás, PhD.

Forma vzdelávania: doktorandské štúdium – externá forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM, FEI STU

Dizertačná skúška: 19.3.2014

Predpokladaný termín ukončenia:

Téma práce: Virtualizácia elektronických služieb

Prerušenie: 01.6.2016 - 31.5.2018

Zanechal: 20.5.2019

VIII.3. Doktorandi vedení pracovními ÚIM na iných pracoviskách

IX. ÚČASŤ PRACOVNÍKOV ÚSTAVU NA KONFERENCIÁCH

IX.1. Zahraničné konferencie

NÁZOV KONFERENCIE : Gamm 2019

Miesto: Viedeň, Rakúsko

Dátum: 18.-22.2.2019

Meno: prof. RNDr. Igor Bock, PhD.

Príspevok: An optimal design with respect to thickness of an elastic plate in dynamic contact with a rigid obstacle

NÁZOV KONFERENCIE : Trendy ve vzdelávaní 2019

Miesto: Velké Losiny

Dátum: 15.-17.5.2019

Meno: Ing. Alexander Hambalík, PhD.

Príspevok: Príprava študentov, odborníkov pre oblasť Biometrie

NÁZOV KONFERENCIE : Workshop Quantum Contextualitz in Quantum Mechanics and Beyond 2019

Miesto: Praha, Česká republika

Dátum: 17.-20.5.2019

Meno: doc. RNDr. Oľga Nánásiová, PhD.

NÁZOV KONFERENCIE : Olomoucké dni aplikovanéj matematiky

Miesto: Olomouc, Česká republika

Dátum: 29.-30.5.2019

Meno: prof. RNDr. Igor Bock, PhD.

Príspevok: A dynamic optimal control problém for an elastic plate in a contact with a rigid obstacle

NÁZOV KONFERENCIE : CECC 2019

Miesto: Telč, Česká republika

Dátum: 11.-14.6.2019

Meno: Ing. Peter Špaček

Príspevok: Quantum resistant handshake: code-based KEM candidates

NÁZOV KONFERENCIE : CECC 2019

Miesto: Telč, Česká republika

Dátum: 11.-14.6.2019

Meno: prof. Ing. Pavol Zajac, PhD.

Príspevok: Code-based signature scheme derived from a MRHS representation of an AES encryption

NÁZOV KONFERENCIE : CECC 2019

Miesto: Telč, Česká republika

Dátum: 11.-14.6.2019

Meno: prof. RNDr. Otokar Grošek, PhD.

NÁZOV KONFERENCIE : CECC 2019

Miesto: Telč, Česká republika

Dátum: 11.-14.6.2019

Meno: Ing. Eugen Antal, PhD.

Príspevok: Solving Historical Ciphers using Evolutionary Programming

NÁZOV KONFERENCIE : MobiCASE 2019, 10th EAI International Conference on Mobile Computing, Applications and Services, IEEE 2019

Miesto: Hangzhou, Čína

Dátum: 13.-20.6.2019

Meno: Ing. Maroš Čavojský, PhD.

Príspevok: Comparison of User Trajectories with the Needleman-Wunsch Algorithm

NÁZOV KONFERENCIE : BFA 2019

Miesto: Florencia, Taliansko

Dátum: 16.-22.6.2019

Meno: prof. Ing. Pavol Zajac, PhD.

Príspevok: Linear and Differential Properties of S-boxes with Respect to Modular Addition

NÁZOV KONFERENCIE : Histocrypt 2019

Miesto: Mons, Belgicko

Dátum: 23.-27.6.2019

Meno: Ing. Eugen Antal, PhD, prof. Ing. Pavol Zajac, PhD., prof. RNDr. Otokar Grošek, PhD.,

Príspevok: Cryptology in the Slovak State During WWII

NÁZOV KONFERENCIE : Petri Nets 2019 a IEEE ACSD 2019

Miesto: Aachen, Nemecko

Dátum: 25.-28.6.2019

Meno: prof. RNDr. Gabriel Juhás, PhD.

NÁZOV KONFERENCIE : Petri Nets 2019 a IEEE ACSD 2019

Miesto: Aachen, Nemecko

Dátum: 25.-28.6.2019

Meno: Ing. Juraj Mažári

NÁZOV KONFERENCIE : IDAACS 2019

Miesto: Metz, Francúzsko

Dátum: 17.-22.9.2019

Meno: Ing. Štefan Balogh, PhD.

NÁZOV KONFERENCIE : Elmar 2019

Miesto: Zadar, Chorvátsko

Dátum: 23.-25.9.2019

Meno: prof. Dr. Ing. Miloš Oravec

Príspevok: Image quality detection using the siamese convolutional neural network

NÁZOV KONFERENCIE : Workshop AWPN 2019

Miesto: Hagen, Nemecko

Dátum: 10.-11.10.2019

Meno: Ing. Milan Mladoniczky

Príspevok: Cluster-Inter proces communication in Petriflow Language

NÁZOV KONFERENCIE : Workshop AWPN 2019

Miesto: Hagen, Nemecko

Dátum: 10.-11.10.2019

Meno: Ing. Juraj Mažári

Príspevok: Execution of Event Chains in a Petriflow Model

NÁZOV KONFERENCIE : Workshop AWPN 2019

Miesto: Hagen, Nemecko

Dátum: 10.-11.10.2019

Meno: prof. RNDr. Gabriel Juhás, PhD.

Príspevok: Implementation Semantics of Petriflow Models

NÁZOV KONFERENCIE : 14° Congreso Interamericano de computacion aplicada a la industria de proceso – CAIP 2019

Miesto: Lima, Peru

Dátum: 21.-24.10.2019

Meno: RNDr. Igor Brilla, PhD.

Príspevok: Numerical Determination of Voltage Potential Inside Nonhomogeneous Media Using Variational Approach

NÁZOV KONFERENCIE : Cyber & AI Prague 2019

Miesto: Praha, Česká republika

Dátum: 24.-26.10.2019

Meno: Ing. Štefan Balogh, PhD., Ing. Peter Švec

Príspevok: Semantic approach for knowledge sharing in security domain

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2019

Miesto: Praha, Česká republika

Dátum: 5.-6.12.2019

Meno: prof. Ing. Pavol Zajac, PhD.

Príspevok: Integration of post-quantum cryptography into Android application

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2019

Miesto: Praha, Česká republika

Dátum: 5.-6.12.2019

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

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2019

Miesto: Praha, Česká republika

Dátum: 5.-6.12.2019

Meno: Ing. Eugen Antal, PhD.

Príspevok: Solving encrypted correspondence of Marie Antoinette

Príspevok: Comparison of vowel identification methods and their use in solving historical ciphers

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2019

Miesto: Praha, Česká republika

Dátum: 5.-6.12.2019

Meno: Ing. Peter Švec

Príspevok: Video Steganography based on Synchronization Timestamps

IX.2. Domáce konferencie

NÁZOV KONFERENCIE : MIST 2019

Miesto: Rajecná Lesná

Dátum: 14.-18.1.2019

Meno: doc. RNDr. Boris Rudolf, PhD.

Príspevok: Set game and Mathematics

NÁZOV KONFERENCIE : Konferencia o eLearningových technológiách a ich aplikáciách
ICETA 2019

Miesto: Starý Smokovec

Dátum: 20.-22.11.2019

Meno: prof. RNDr. Gabriel Juhás, PhD.

NÁZOV KONFERENCIE : Konferencia o eLearningových technológiách a ich aplikáciách
ICETA 2019

Miesto: Starý Smokovec

Dátum: 20.-22.11.2019

Meno: Ing. Juraj Mažári

NÁZOV KONFERENCIE : Konferencia o eLearningových technológiách a ich aplikáciách
ICETA 2019

Miesto: Starý Smokovec

Dátum: 20.-22.11.2019

Meno: Ing. Milan Mladoniczky

X. HABILITAČNÉ A INAUGURAČNÉ KONANIA

X.1. Inauguračné konania

X.2. Habilitačné konania

X.3. Členstvá v komisiách

prof. RNDr. Otokar Grošek, PhD.: účasť na habilitačnej prednáške Petra Švendu, Fakulta informatiky MU, Brno, ČR 26.3.2019

prof. RNDr. Gabriel Juhás, PhD.: oponent inauguračnej práce doc. Cimráka, Žilinská univerzita (21.1.2019)

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

XI.1. Obhajoby dizertačných prác na ÚIM

Ing. Dominik Sopiak: Návrh multimodálneho biometrického systému,
školiteľ prof. Dr. Ing. M. Oravec, 17.1.2019

Ing. Juraj Varga: Bezpečnosť mobilných zariadení
školiteľ prof. Ing. P. Zajac, PhD., 18.1.2019

Ing. Maroš Čavojský: Metodológia a systém na efektívne testovanie mobilných aplikácií
školiteľ Dr.rer.nat. M. Drozda, PhD., 1.7.2019

Ing. Igor Kazlov: Analýza udalostných systémov s viacerými inštanciami
školiteľ prof. RNDr. G. Juhás, PhD., 26.8.2019

XI.2. Dizertačné skúšky na ÚIM

Ing. Zuzana Bukovčíková 15.3.2019, školiteľ prof. Dr. Ing. M. Oravec

Ing. Juraj Mažári 3.6.2019, školiteľ prof. RNDr. G. Juhás, PhD.

Ing. Milan Mladoniczky 3.6.2019, školiteľ prof. RNDr. G. Juhás, PhD.

Ing. Peter Špaček 7.5.2019, školiteľ prof. Ing. P. Zajac, PhD.

XI.3. Členstvá v komisiách

prof. RNDr. Otokar Grošek, PhD.: predseda dizertačnej komisie pri obhajobe Ing. D. Sopiaka (17.1.2019), Ing. J. Vargu (18.1.2019) a Ing. I. Kazlova (26.8.2019), člen diz. Komisie pri obhajobe Ing. M. Čavojského (1.7.2019)

prof. RNDr. Igor Bock, PhD.: člen komisie na obhajobu dizertačnej práce Mgr. Mariána Šagáta (obhájená 26.8.2019 na Katedre matematiky a deskriptívnej geometrie, SvF STU)

XI.4. Dizertačné skúšky a obhajoby dizertačných prác na iných pracoviskách

prof. RNDr. Igor Bock, PhD.: práca Mgr. Izabely Riečanovej s názvom *Numerical methods and their use in acoustical simulations* (obhájená 27.5.2019 na Katedre matematiky a deskriptívnej geometrie, SvF STU)

XI.5. Oponentské posudky k dizertačnej práci

XI.6. Skúšky doktorandov z doktorandských predmetov

Meno Doktoranda	Odbor štúdia	Meno skúšajúceho	Predmet	Dátum

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

XII.1. ŠVOČ

Komisia spoločná s ÚMIKT: predseda: Prof. RNDr. Gabriel Juhás, PhD.

členovia: doc. Ing. Miloš Orgoň, PhD.

Ing. Viliam Hromada, PhD.

Ing. Tomáš Páleník, PhD.

Tajomník: Ing. Vladislav Novák

Meno študenta ÚIM	Roč.	Názov práce	Vedúci
Ivan Kováč	3.BŠ	Multimodal biometric system based on fingerprint and fingern vein pattern	Ing. P. Marák
Michal Firča	3.BŠ	Porovnanie metód identifikácie samohlások v texte	Ing. E. Antal, PhD.
Bc. Tomáš Stanko	2.IŠ	Rotačná vzdialenosť binárných vyhľadávacích stromov	doc. Ing. M. Vojvoda, PhD.

Meno: prof. RNDr. Igor Bock, PhD.

Člen komisie pre posúdenie prác Študentskej vedeckej konferencie na Staveb. Fak. STU v sekcii Matematické a počítačové modelovanie, 25.4.2019

XII.2. VEDENIE UKONČENÝCH DIPLOMOVÝCH PRÁC

Baka Tomáš, Bc.	Riešenie MRHS rovníc cez dekodovacie algoritmy	P. Zajac
Bako Juraj, Bc.	Systém pre rozšírenú realitu s využitím OpenGL	M. Drozda
Baraniak Tomáš, Bc.	Dekódovanie QC-MDPC kódov	T. Fabšič
Biačko Ivan, Bc.	Rozšírená realita pre Android	M. Drozda
Biely Martin, Bc.	Mobilná aplikácia na platforme Android pre zobrazovanie parametrov mechatronického vozidla prenášaných pomocou rozhrania Bluetooth	P. Fuchs
Bucsai Szabina, Bc.	Ovládanie a monitorovanie IoT zariadení s využitím zmiešanej reality	E. Kučera
Dačo Pavol, Bc.	Návrh algoritmu pre predikciu poškodenia poľnohospodárskych plodín	M. Jagelka
Danko Roman, Bc.	SSH autentifikácia s použitím osobitných kľúčov spravovaných v krypto peňaženke Trezor	M. Jókay
Dičér Andrej, Bc.	Tvorba mobilnej aplikácie pre riadenie vozidla s využitím React Native	P. Bisták
Dobrovodský Martin, Bc.	Informačný systém na sprístupnenie informácií ohľadne fungovania zdravotníctva v Slovenskej republike	A. Hambalik
Dubeň Andrej, Bc.	Rozpoznávanie osôb na historických fotografiách	M. Oravec
Džáčovský Matúš, Bc.	Vývoj webových aplikácií na princípe RESTfull servisov	O. Gallo
Džadoň Tomáš, Bc.	Návrh algoritmu pre energeticky efektívny senzorický bod	M. Jagelka
Filo Róbert, Bc.	Aplikácia pre Internet of Things využívajúca Low-Power Wide-Area Network	E. Kučera
Gburík Martin, Bc.	Manažment zmien medzi verziovanými procesmi Petriho sietí	G. Juhás
Hvozdík Milan, Bc.	Evolúcia umelého života	I. Sekaj
Chalány Michal, Bc.	Salomaa-Welzl kryptosystém	O. Grošek
Chlebovec Martin, Bc.	Prezentácia produktov v e-commerce prostredí s využitím rozšírenej reality	O. Haffner
Jahodníková Barbora, Bc.	Tlač fotografií pomocou súradnicového zapisovača	P. Ťapák
Kanás Ján, Bc.	Strojové učenie pri klasifikácii máp význačnosti	R. Vargic
Kováč Ján, Bc.	Reakčný útok na QC-MDPC McEliece kryptosystém	T. Fabšič

Kostuňová Alena, Bc.	Využitie metód výpočtovej inteligencie na vyhodnocovanie kvality zvarov	E. Kučera
Krkoška Marián, Bc.	Bezpečná geolokácia	P. Zajac
Kubričan Juraj, Bc.	Automatizované generovanie aplikačného rozhrania v procesne orientovaných systémoch	G. Juhás
Kurt'ák Adam, Bc.	Rozvrhový systém pre FEI - frontend	M. Jókay
Kvočka Roman, Bc.	Extrakcia obrazových príznakov založená na posilňovanom učení	J. Pavlovičová
Kysel' Peter, Bc.	Implementácia HFE kryptosystému pre konečné polia $GF(2^k)$ a $GF(p)$	V. Hromada
Kytková Emília, Bc.	Rozpoznávanie osôb v čase	M. Oravec
Lukáč Matúš, Bc.	Detegovanie významných tvárových charakteristík / doplnkov	D. Sopiak
Makšin Martin, Bc.	Rozvrhový systém pre FEI - backend	M. Jókay
Matalíková Katarína, Bc.	Vyhľadávanie nad zašifrovanými dátami	M. Vojvoda
Mášiková Andrea, Bc.	Android hra pre zlepšenie reakčných schopností	S. Marček
Michalica Tomáš, Bc.	Transformácia procesného modelu na textovú reprezentáciu	G. Juhás
Michňa Michal, Bc.	Využitie technológií sémantického webu v oblasti cestovného ruchu	I. Kossaczky
Molčan Lukáš, Bc.	Rozšírená realita pre Android	M. Drozda
Mužila Lukáš, Bc.	Využitie MDA princípov vo vývoji aplikácii pre internet vecí	O. Gallo
Novotný Martin, Bc.	Implementácia experimentálneho postkvantového protokolu	P. Zajac
Ogurčák Samuel, Bc.	Android hra pre zlepšenie reakčných schopností	S. Marček
Páleník Rastislav, Bc.	Implementácia EFC kryptosystému pre konečné polia $GF(2^k)$ a $GF(p)$	V. Hromada
Pažitný Peter, Bc.	Automatizácia pracoviska a spracovanie meraných dát v programovom prostredí LabView	J. Kováč
Pernický Ľubor, Bc.	Využitie postkvantovej kryptografie na Android platforme	P. Zajac
Podhorec Samuel, Bc.	Niemiho kryptosystém	V. Hromada
Podlucky Filip, Bc.	Web aplikácia pre sledovanie pohyblivého cieľa	K. Žáková
Pochybová Lucia, Bc.	React komponent pre webovú aplikáciu na testovanie úrovne softvérových vývojárov	M. Kocúr
Rajnič František, Bc.	Návrh a realizácia kompresného algoritmu pre dáta zo zariadenia na zisťovanie polohy	M. Jagelka
Rences Tomáš, Bc.	Návrh metodiky optimálneho plánovania pracovných činností	I. Sekaj
Román Róbert, Bc.	Inteligentný diagnostický systém na platforme Windows	Š. Bucz
Sahul Dušan, Bc.	Rozpoznávanie aktivity vo videu	D. Sopiak
Slezák Michal, Bc.	Využitie zmiešanej reality na ovládanie a monitorovanie mechatronických zariadení	O. Haffner
Stanko Tomáš, Bc.	Rotačná vzdialenosť binárnych stromov	M. Vojvoda
Šašala Štefan, Bc.	Využitie VR pri experimentoch	E. Stuchlíková
Šefčík Ivan, Bc.	Komplexný systém pre výkon skúšok odolnosti voči spojitému rušeniu	J. Hallon
Šimčíková Simona, Bc.	Manažment pacientov na centrálnom prijme	A. Hambalik
Šulák Patrik, Bc.	Informačný systém na spracovanie údajov znečistenia životného prostredia	M. Vojs

Švec Peter, Bc.	Rozšírenie knižnice StegoDisk	M. Jókay
Trocha Martin, Bc.	Tvorba API pre online prístup k simulačnému prostrediu Matlab	K. Žáková
Ujmiak Branislav, Bc.	Využitie telemedicínskych služieb v starostlivosti o starších ľudí	A. Hambalik
Urban Kristína, Bc.	Určovanie veku osôb z fotografie	M. Oravec
Valašík Adam, Bc.	Aplikácia pre Internet of Things využívajúca Sigfox protokol	E. Kučera
Vasíľ Marcel, Bc.	Rozoznávanie geografických bodov na obraze	D. Sopiak
Vizváry Ladislav, Bc.	Detekcia kvality obrazu	D. Sopiak
Vrabec Juraj, Bc.	Univerzálne komunikačné rozhranie pre internet vecí	O. Gallo
Zelenčík Michal, Bc.	Pokrytie sieťovej komunikácie v LSM Medusa	M. Jókay

XII.3. ČLENSTVO V ŠTÁTNICOVÝCH KOMISIÁCH

Meno	Bc. 11.6.	Bc. 2.-3.7.	Ing. 10.-11.-12.6.	Iné
E. Antal	X	X	X	
Š. Balogh		X X	X	
Z. Bukovčíková		X	X	
I. Brilla				
K. Čipková		X	X	
M. Drozda		X	X X	
T. Fabšič		X X	X X	
O. Gallo		X X	X X	
O. Grošek	X	X	X X	
A. Hambalík		X	X	
V. Hromada		X X	X X	
M. Jókay	X	X X	X	
G. Juhás		X X	X X	FIIT
M. Kečkemétyová				
J. Kollár			X	
I. Kossaczký	X	X X	X	
P. Marák		X		
S. Marček		X X	X X	
I. Marinová			X	
E. Marko		X	X	
J. Mažári		X X	X X	
M. Mladoniczky		X X	X X	
O. Nánásiová		X	X	
K. Nemoga		X	X	
V. Novák	X	X	X	
M. Oravec			X	

D. Pancza			X	
E. Pastuchová		X		
M. Polakovič			X	
R. Ploszek		X	X	X
B. Rudolf		X		
D. Sopiak		X		X
P. Špaček		X	X	X
M. Šrámka			X	X
M. Vojvoda		X	X	X
M. Zajac		X	X	X
P. Zajac		X	X	X
M. Zákopčan		X	X	

XIII. EDIČNÉ AKTIVITY

XIII.1. Vydávanie časopisov

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

XIII.1.1 Editované čísla v roku 2019

prof. RNDr. Otokar Grošek, PhD.

Editor: Number Theory, algebra and and Cryprology '18. Tatra Mountains Mathematical Pub. Vol. 73, 2019.

XIII.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. Oľga Nánásiová, PhD.** je členka redakčnej rady Forum Statisticum Slovaca
- **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)

XIII.3. Recenzie pre vedecké časopisy, knihy, zborníky a učebnice

prof. RNDr. Igor Bock, PhD. – 1. Zeitschrift für Angew. Math. und Mech. – 1 recenzia
2. Applications of Mathematics – 1 recenzia
3. Mathematical Reviews – 11 prehľadov
6. Zentralblatt für Mathematik – 17 prehľadov

prof. RNDr. Otokar Grošek, PhD.: Journal of Combinatorial Design – 2 recenzie
Tatra Mountains Math. Publ. – 1 recenzia

doc. RNDr. Boris Rudolf, PhD.: Vydavateľstvo UK, 1 recenzia skript

doc. Ing. Milan Vojvoda PhD.: Tatra Mountains Math. Publ. – 1 recenzia

XIII.4. Recenzie príspevkov na vedecké konferencie

prof. RNDr. Otokar Grošek, PhD.: recenzia príspevky na CECC 2019

XIII.5. Recenzie vedeckých projektov

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

doc. RNDr. Boris Rudolf, PhD. – Projekt VEGA – 1 recenzia

XIV. ORGANIZÁCIA KONFERENCIÍ, ČLENSTVÁ VO VÝBOROCH

NÁZOV KONFERENCIE : International Conference on Historical Cryptology

Miesto: Mons, Belgicko

Dátum: 23.-26.6.2019

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

Funkcia: člen programového výboru

XV. SEMINÁRE

Seminár: VARIÁČNÉ NEROVNICE A OPTIMÁLNE RIADENIE V MECHANIKE

Vedúci: prof. RNDr. Igor Bock, PhD.

Seminár: CRYPTO

Vedúci: prof. Ing. Pavol Zajac, PhD.

Seminár: MACHINE LEARNING

Vedúci: prof. Dr. Ing. Miloš Oravec

Seminár: APLIKÁCIE MATEMATIKY
vedúci: doc. RNDr. Oľga Nánásiová, PhD.