O Z N A M

Vo výberovom konaní vyhlásenom dekanom Fakulty elektrotechniky a informatiky STU v Bratislave, ktoré sa konalo dňa 27.04.2023 na obsadenie :

- **1 pracovného miesta *odborného asistenta*** pre študijný odbor **Informatika** na Ústav informatiky a matematiky FEI STU od 1.5.2023 uspel:

Mgr. Tomáš Fabšič, PhD.

Zoznam členov výberovej komisie v rozsahu meno a priezvisko:

Martin Weis

Martin Drozda

Oľga Nánásiová

Milan Vojvoda

Danica Rosinová

Údaje vybraného uchádzača:

Meno, priezvisko, rodné priezvisko: Tomáš Fabšič, Fabšič

Akademické tituly, vedecko-pedagog. tituly, umelecko-pedagog. tituly, vedecké hodnosti:

Mgr., PhD.

Rok narodenia: 1986

Údaje o vysokoškolskom vzdelaní, ďalšom akademickom raste a absolvovanom ďalšom vzdelávaní:

[2013 – 2017] PhD. v aplikovanej informatike

FEI STU v Bratislave

[2011 – 2013] Mgr. v matematike

FMFI UK v Bratislave

Ilkovičova 3
812 19 Bratislava
www.stuba.sk

sona.mikusova@stuba.sk
T: +4212 60291 681

[2009 – 2010] Master of Advanced Study in Mathematics

University of Cambridge

Adresa: Spojené kráľovstvo [2006 – 2009] BSc. in Mathematics

University of Warwick

Adresa: Spojené kráľovstvo

Údaje o priebehu zamestnaní a priebehu pedagogickej činnosti:

[2023 – Súčasné zamestnanie]

VEGA 1/0105/23 Postkvantová kryptografia odolná voči postranným kanálom

- zástupca vedúceho projektu

[2023 – Súčasné zamestnanie]

NATO SPS Project G5985 Secure Communication via Classical and Quantum Technologies

- člen riešiteľského kolektívu

[2021 – Súčasné zamestnanie]

APVV-19-0436 Nové informačné a komunikačné technológie pre budúcu informačnú infraštruktúru

- člen riešiteľského kolektívu

[2018 – 2022] NATO SPS Project G5448 Secure Communication in the Quantum Era

- člen riešiteľského kolektívu

[2017 – 2020] VEGA 1/0159/17 Bezpečná postkvantová kryptografia

- člen riešiteľského kolektívu

[2015 – 2016] NATO SfP 984520 Secure Implementation of Post-Quantum Cryptography

- člen riešiteľského kolektívu

[2015 – 2016] SK06-IV-01-001 Kryptografia prináša bezpečnosť a slobodu

- člen riešiteľského kolektívu

[2015 – 2015] VEGA 1/0173/13 Ochrana osobných údajov v mobilných zariadeniach

- člen riešiteľského kolektívu

Údaje o odbornom alebo umeleckom zameraní:

ČLENSTVO V ORGANIZÁCIÁCH A SIEŤACH

[15.02.2023 – Súčasné zamestnanie] Pracovná skupina pre vedu, výskum, a inovácie FEI STU - člen

[05.01.2022 – Súčasné zamestnanie] Pracovná skupina pre posúdenie súladu študijného programu Aplikovaná informatika na FEI STU so štandardmi pre študijný program - člen

VYZNAMENANIA A OCENENIA

[2017] Študentská osobnosť Slovenska akad.r. 2016/2017, absolútny víťaz Udeľujúca inštitúcia: JCI-Slovensko

[2017] Študentská osobnosť Slovenska akad.r. 2016/2017, víťaz v kategórii Informatika a matematicko-fyzikálne vedy Udeľujúca inštitúcia: JCI-Slovensko

[2017] Študent roka 2017 Udeľujúca inštitúcia: STU v Bratislave Ocenenie od rektora STU v Bratislave za mimoriadny výsledok v oblasti výskumu a vývoja.

[2009] Gates Cambridge Scholarship 2009/2010 Udeľujúca inštitúcia: Bill & Melinda Gates Foundation Štipendium od nadácie Bill & Melinda Gates Foundation pokrývajúce náklady spojené so štúdiom na University of Cambridge.

[2009] The University of Warwick Mathematics Institute Mathematics BSc Prize 2009 Udeľujúca inštitúcia: Mathematics Institute, University of Warwick Ocenenie za vynikajúce študijné výsledky.

[2009] IBM Student Recognition Award 2009 Udeľujúca inštitúcia: IBM Ocenenie za vynikajúce študijné výsledky.

[2008] The University of Warwick Mathematics Institute 2nd Year Mathematics Prize 2008 Udeľujúca inštitúcia: Mathematics Institute, University of Warwick Ocenenie za vynikajúce študijné výsledky.

Údaje o publikačnej činnosti:

V2 Vedecký výstup publikačnej činnosti ako časť editovanej knihy alebo zborníka

V2_01 ABELA, Robert - COLOMBO, Christian - MALO, Peter - SÝS, Peter - FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam - VELLA, Mark. Secure implementation of a quantum-future GAKE protocol. In ZHOU, Jianying.*Security and Trust Management : 17th International Workshop, STM 2021. Darmstadt, Germany. October 8, 2021*. Cham : Springer, 2021, S. 103-121. ISBN 978-3-030-91858-3. V databáze: DOI: 10.1007/978-3-030-91859-

0_6 ; SCOPUS: 2-s2.0-85121907279.
Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_02 FABŠIČ, Tomáš - GALLO, Ondrej. Acoustic cryptanalysis. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 34-38. ISBN 978-80-227-4541-3.
Kategória publikácie do 2021: AFC

V2_03 FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam. Simple power analysis on the McEliece cryptosystem on STM32F4 and Altera cyclone. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 57-58. ISBN 978-80-227-4541-3.
Kategória publikácie do 2021: AFG

V2_04 FABŠIČ, Tomáš - HROMADA, Viliam - STANKOVSKI, Paul - ZAJAC, Pavol - GUO, Qian - JOHANSSON, Thomas. A reaction attack on the QC-LDPC McEliece cryptosystem. In *Post-quantum cryptography : 8th International conference. Utrecht, The Netherlands. June 26-28, 2017*. Cham : Springer, 2017, S. 51-68. ISBN 978-3-319-59878-9. V databáze: SCOPUS: 2-s2.0-85021776403.
Kategória publikácie do 2021: AFC

V2_05 FABŠIČ, Tomáš - HROMADA, Viliam - ZAJAC, Pavol. Reaction attacks on cryptosystems using QC-LDPC codes. In *CECC 2018 : Central European conference on cryptology. Smolenice, Slovakia. June 6-8, 2018*. Bratislava : Slovak Academy of Sciences, 2018, S. 62-63. ISBN 978-80-968374-5-8.
Kategória publikácie do 2021: AFD

V3 Vedecký výstup publikačnej činnosti z časopisu

V3_01 FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam. Simple power analysis attack on the QC-LDPC McEliece cryptosystem. In *Tatra Mountains Mathematical Publications*. Vol. 67, (2016), s. 85-92. ISSN 1210-3195 (2016: 0.367 - SJR, Q3 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85014730719.
Kategória publikácie do 2021: ADN

V3_02 FABŠIČ, Tomáš - GROŠEK, Otokar - NEMOGA, Karol - ZAJAC, Pavol. On generating invertible circulant binary matrices with a prescribed number of ones. In *Cryptography and Communications*. Vol. 10, Iss. 1 (2018), s. 159-175. ISSN 1936-2447 (2018: 1.099 - IF, Q2 - JCR Best Q, 0.547 - SJR, Q2 -

SJR Best Q). V databáze: SCOPUS: 2-s2.0-85041074817 ; CC: 000428746900011.
Kategória publikácie do 2021: ADC

V3_03 GROŠEK, Otokar - FABŠIČ, Tomáš. Computing multiplicative inverses in finite fields by long division. In *Journal of Electrical Engineering*. Vol. 69, No. 5 (2018), s. 400-402. ISSN 1335-3632 (2018: 0.636 - IF, Q4 - JCR Best Q, 0.200 - SJR, Q3 - SJR Best Q). V databáze: WOS: 000453413200012 ; SCOPUS: 2-s2.0-85059569379.
Kategória publikácie do 2021: ADN

V3_04 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 (2019: 0.432 - IF, Q3 - JCR Best Q, 0.106 - SJR, Q4 - SJR Best Q). V databáze: CC: 000469567400001 ; DOI: 10.1080/01611194.2019.1596997.
Kategória publikácie do 2021: ADC

O2 Odborný výstup publikačnej činnosti ako časť knižnej publikácie alebo zborníka

O2_01 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.
Kategória publikácie do 2021: BFA

O2_02 FABŠIČ, Tomáš. A reaction attack on LEDApkc. In *CBC 2018 : The Sixth Code-Based Cryptography Workshop. Abstracts. Davie, Florida, USA. April 5-6, 2018*. Florida : Atlantic University, 2018, [1] s.
Kategória publikácie do 2021: BFA

I1 Iný výstup publikačnej činnosti ako celok

I1_01 FABŠIČ, Tomáš. *Contributions to the Analysis of the QC-LDPC McEliece Cryptosystem : dát. obhaj. 23.11.2017, č. ved. odboru 9-2-9*. 2017. 119 s. Dostupné na internete: <http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=130770>.
Kategória publikácie do 2021: DAI

I2 Iný výstup publikačnej činnosti ako časť publikácie alebo zborníka

I2_01 FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam. Demonstration of acoustic cryptanalysis. In *CryptArchi 2017 [elektronický zdroj] : 15th International workshop on cryptographic architectures embedded in logic devices. Smolenice, Slovakia. June 18-21, 2017*. Saint-Étienne : Laboratoire Hubert Curien, 2017, online, S. 11.
Kategória publikácie do 2021: GHG

I2_02 FABŠIČ, Tomáš - GALLO, Ondrej - GROŠEK, Otokar - HROMADA, Viliam - ZAJAC, Pavol. Post-quantum cryptography research at UIM FEI STU. In *Kvantové rendezvous : Smolenice. 29.6.-1.7.2022*, [5] s.
Typ výstupu: časti, ktoré nemožno zaradiť do kategórie V, O, P, U alebo D; Výstup: domáci; Kategória publikácie do 2021: GII

Ohlasy na vedeckú alebo umeleckú prácu:

V2 Vedecký výstup publikačnej činnosti ako časť editovanej knihy alebo zborníka

V2_01 ABELA, Robert - COLOMBO, Christian - MALO, Peter - SÝS, Peter - FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam - VELLA, Mark. Secure implementation of a quantum-future GAKE protocol. In ZHOU, Jianying.*Security and Trust Management : 17th International Workshop, STM 2021. Darmstadt, Germany. October 8, 2021*. Cham : Springer, 2021, S. 103-121. ISBN 978-3-030-91858-3. V databáze: DOI: 10.1007/978-3-030-91859-0_6 ; SCOPUS: 2-s2.0-85121907279.
Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_02 FABŠIČ, Tomáš - GALLO, Ondrej. Acoustic cryptanalysis. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 34-38. ISBN 978-80-227-4541-3.
Kategória publikácie do 2021: AFC

V2_03 FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam. Simple power analysis on the McEliece cryptosystem on STM32F4 and Altera cyclone. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 57-58. ISBN 978-80-227-4541-3.
Kategória publikácie do 2021: AFG
Ohlasy:
1. [1] GUO, Ying - OU, Yu - LI, Lang. Construction of a high efficient distinguisher in differential power analysis attacks. In Proceedings of

Science, 2017-01-01, 2017-December, pp., Registrované v: SCOPUS
Ohlas: zahraničný
2. [1] BALDI, Marco - BARENGHI, Alessandro - CHIARALUCE, Franco - PELOSI, Gerardo - SANTINI, Paolo. LEDAkem: A post-quantum key encapsulation mechanism based on QC-LDPC Codes. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018-01-01, 10786 LNCS, pp. 3-24. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
3. [1] SANTINI, Paolo - BATTAGLIONI, Massimo - CHIARALUCE, Franco - BALDI, Marco. Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019-01-01, 11666 LNCS, pp. 115-136. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný

V2_04 FABŠIČ, Tomáš - HROMADA, Viliam - STANKOVSKI, Paul - ZAJAC, Pavol - GUO, Qian - JOHANSSON, Thomas. A reaction attack on the QC-LDPC McEliece cryptosystem. In *Post-quantum cryptography : 8th International conference. Utrecht, The Netherlands. June 26-28, 2017*. Cham : Springer, 2017, S. 51-68. ISBN 978-3-319-59878-9. V databáze: SCOPUS: 2-s2.0-85021776403.
Kategória publikácie do 2021: AFC
Ohlasy:
1. [1] BALDI, Marco. Post-quantum cryptographic schemes based on codes. In Proceedings 2017 International Conference on High Performance Computing and Simulation, HPCS 2017, 2017-09-12, pp. 908-910., Registrované v: SCOPUS, WOS
Ohlas: zahraničný
2. [1] DRAGOI, Vlad - KALACHI, Herve Tale. Cryptanalysis of a Public Key Encryption Scheme Based on QC-LDPC and QC-MDPC Codes. In IEEE COMMUNICATIONS LETTERS, 2018, vol. 22, no. 2, pp. 264-267. ISSN 1089-7798., Registrované v: WOS, SCOPUS
Ohlas: zahraničný
3. [1] BALDI, Marco - SANTINI, Paolo - CANCELLIERI, Giovanni. Post-quantum cryptography based on codes: state of the art and open challenges. In 2017 AEIT INTERNATIONAL ANNUAL CONFERENCE, 2017, vol., no., pp., Registrované v: WOS, SCOPUS
Ohlas: zahraničný
4. [1] EATON, Edward - LEQUESNE, Matthieu - PARENT, Alex - SENDRIER, Nicolas. QC-MDPC: A timing attack and a CCA2 KEM. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018-01-01, 10786 LNCS, pp. 47-76. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný

5. [1] BALDI, Marco - BARENGHI, Alessandro - CHIARALUCE, Franco - PELOSI, Gerardo - SANTINI, Paolo. LEDAkem: A post-quantum key encapsulation mechanism based on QC-LDPC Codes. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018-01-01, 10786 LNCS, pp. 3-24. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
6. [1] SANTINI, Paolo - BALDI, Marco - CANCELLIERI, Giovanni - CHIARALUCE, Franco. Hindering Reaction Attacks by Using Monomial Codes in the McEliece Cryptosystem. In IEEE International Symposium on Information Theory Proceedings, 2018-08-15, 2018-June, pp. 951-955. ISSN 21578095., Registrované v: SCOPUS
Ohlas: zahraničný
7. [1] PAIVA, Thales Bandiera - TERADA, Routo. Improving the effciency of a reaction attack on the QC-MDPC McEliece. In IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018-10-01, e101A, 10, pp. 1676-1686. ISSN 09168508., Registrované v: SCOPUS
Ohlas: zahraničný
8. [1] BAGHERI, Khadijeh - SADEGHI, Mohammad-Reza - EGHLIDOS, Taraneh. An Efficient Public Key Encryption Scheme Based on QC-MDPC Lattices. In IEEE ACCESS, 2017, vol. 5, no., pp. 25527-25541. ISSN 2169-3536., Registrované v: WOS, SCOPUS
Ohlas: zahraničný
9. [1] SANTINI, Paolo - BALDI, Marco - CHIARALUCE, Franco. Assessing and countering reaction attacks against post-quantum public-key cryptosystems based on QC-LDPC codes. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018-01-01, 11124 LNCS, pp. 323-343. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
10. [1] FARKAŠ, Peter. Two Countermeasures against Reaction Attacks on LEDApkc and other QC-MDPC and QC-LDPC based McEliece Cryptosystems in ARQ Setting : Heuristic Discussion. In SoftCOM 2018 : 26th International conference on software, telecommunications and computer networks. Split, Croatia. September 13-15, 2018. 1. ed. Split : University of Split, 2018, S. 128-132. ISSN 2623-6559., Registrované v: WOS, SCOPUS
Ohlas: zahraničný
11. [1] FARKAŠ, Peter. Further heuristic discussion on two countermeasures against reaction attacks on McEliece cryptosystems with QCLDPC codes. In EST 2019 : Eighth International Conference on Emerging Security Technologies. Colchester, UK. 22-24 July 2019. 1. ed. Piscataway : IEEE, 2019, Art. no. 01, [4 s.]. ISSN 2472-7601. ISBN 978-1-7281-5546-3., Registrované v: SCOPUS
Ohlas: zahraničný
12. [1] DÖMÖSI, Pál - HANNUSCH, carolin - HORVÁTH, Géza. A

cryptographic System Based on a new class of Binary Error-correcting codes. In Tatra Mountains Mathematical Publications, 2019-08-01, 73, 1, pp. 83-96. ISSN 12103195., Registrované v: SCOPUS
Ohlas: zahraničný
13. [1] BALDI, Marco - BARENGHI, Alessandro - CHIARALUCE, Franco - PELOSI, Gerardo - SANTINI, Paolo. LEDAcrypt: QC-LDPC code-based cryptosystems with bounded decryption failure rate. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019-01-01, 11666 LNCS, pp. 11-43. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
14. [1] SANTINI, Paolo - BATTAGLIONI, Massimo - CHIARALUCE, Franco - BALDI, Marco. Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019-01-01, 11666 LNCS, pp. 115-136. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
15. [1] GUO, Qian - JOHANSSON, Thomas - YANG, Jing. A novel CCA attack using decryption errors against LAC. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019-01-01, 11921 LNCS, pp. 82-111. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
16. [1] HU, Jingwei - BALDI, Marco - SANTINI, Paolo - ZENG, Neng - LING, San - WANG, Huaxiong. Lightweight Key Encapsulation Using LDPC Codes on FPGAs. In IEEE TRANSACTIONS ON COMPUTERS, 2020, vol. 69, no. 3, pp. 327-341. ISSN 0018-9340., Registrované v: WOS, CC, SCOPUS
Ohlas: zahraničný
17. [1] SANTINI, Paolo - BALDI, Marco - CHIARALUCE, Franco. Complexity of statistical attacks on QC-LDPC code-based cryptosystems. In IET Information Security, 2020-05-01, 14, 3, pp. 304-312. ISSN 17518709., Registrované v: SCOPUS
Ohlas: zahraničný
18. [1] WANG, Luping - CHEN, Jie - ZHANG, Kai - QIAN, Haifeng. A post-quantum hybrid encryption based on QC-LDPC codes in the multi-user setting. In Theoretical Computer Science, 2020-01-01, pp. ISSN 03043975., Registrované v: SCOPUS
Ohlas: zahraničný
19. [1] COLOMBO, Christian - VASCO, María Isabel González - STEINWANDT, Rainer - ZAJAC, Pavol. Secure Communication in the Quantum Era: (Group) Key Establishment. In NATO Science for Peace and Security Series B: Physics and Biophysics, 2020-01-01, pp. 65-74. ISSN 18746500., Registrované v: SCOPUS
Ohlas: zahraničný
20. [1] LI, Zhe - HAN, Yiliang - LI, Yu - ZHU, Shuaishuai - YANG,

Xiaoyuan. An overview of code-based encryption schemes. In Guofang Keji Daxue Xuebao/Journal of National University of Defense Technology, 2020-08-28, 42, 4, pp. 134-142. ISSN 10012486., Registrované v: SCOPUS
Ohlas: zahraničný
21. [1] SANTINI, Paolo - BATTAGLIONI, Massimo - BALDI, Marco - CHIARALUCE, Franco. Analysis of the Error Correction Capability of LDPC and MDPC Codes Under Parallel Bit-Flipping Decoding and Application to Cryptography. In IEEE TRANSACTIONS ON COMMUNICATIONS, 2020, vol. 68, no. 8, pp. 4648-4660. ISSN 0090-6778., Registrované v: WOS, CC, SCOPUS
Ohlas: zahraničný
22. [1] CINI, Valerio - RAMACHER, Sebastian - SLAMANIG, Daniel - STRIECKS, Christoph. CCA-Secure (Puncturable) KEMs from Encryption with Non-Negligible Decryption Errors. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2020-01-01, 12491 LNCS, pp. 159-190. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
23. [1] GUO, Qian - JOHANSSON, Thomas. A New Decryption Failure Attack Against HQC. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2020-01-01, 12491 LNCS, pp. 353-382. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
24. [1] SHIMA, Koji - DOI, Hiroshi. New proof techniques using the properties of circulant matrices for xor-based (K, n) threshold secret sharing schemes. In Journal of Information Processing, 2021-01-01, 29, pp. 266-274. ISSN 03875806., Registrované v: SCOPUS
Ohlas: zahraničný
25. [1] FREUDENBERGER, Jürgen - THIERS, Johann Philipp. A new class of q-ary codes for the mceliece cryptosystem. In Cryptography, 2021-03-01, 5, 1, pp., Registrované v: SCOPUS
Ohlas: zahraničný
26. [1] SHUKUR, Wisam Abed - BADRULDDIN, Ahmed - NSAIF, Mohammed Kamal. A proposed encryption technique of different texts using circular link lists. In Periodicals of Engineering and Natural Sciences, 2021-01-01, 9, 2, pp. 1115-11123., Registrované v: SCOPUS
Ohlas: zahraničný
27. [1] SANTINI, Paolo - PERSICHETTI, Edoardo - BALDI, Marco. Reproducible families of codes and cryptographic applications. In Journal of Mathematical Cryptology, 2021-01-01, 16, 1, pp. 20-48. ISSN 18622976., Registrované v: SCOPUS
Ohlas: zahraničný
28. [1] THIERS, Johann Philipp - FREUDENBERGER, Jürgen. Generalized concatenated codes over gaussian and eisenstein integers for code-based cryptography. In Cryptography, 2021-12-01, 5, 4, pp.,

Registrované v: SCOPUS
Ohlas: zahraničný
29. [1] THIERS, Johann Philipp - FREUDENBERGER, Jurgen. Generalized Concatenated Codes over Gaussian Integers for the McEliece Cryptosystem. In IEEE International Conference on Consumer Electronics Berlin, ICCE-Berlin, 2021-01-01, 2021-November, pp. ISSN 21666814., Registrované v: SCOPUS
Ohlas: zahraničný
30. [1] LIU, Jie - TONG, Xiaojun - WANG, Zhu - ZHANG, Miao - MA, Jing. An improved McEliece cryptosystem based on QC-MDPC code with compact key size. In Telecommunication Systems, 2022-01-01, pp. ISSN 10184864., Registrované v: SCOPUS
Ohlas: zahraničný
31. [1] PAIVA, Thales B. - TERADA, Routo. Faster Constant-Time Decoder for MDPC Codes and Applications to BIKE KEM. In: IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022-08-31, 2022, 4, pp. 110-134., Registrované v: SCOPUS
Ohlas: zahraničný

V2_05 FABŠIČ, Tomáš - HROMADA, Viliam - ZAJAC, Pavol. Reaction attacks on cryptosystems using QC-LDPC codes. In *CECC 2018 : Central European conference on cryptology. Smolenice, Slovakia. June 6-8, 2018*. Bratislava : Slovak Academy of Sciences, 2018, S. 62-63. ISBN 978-80-968374-5-8.
Kategória publikácie do 2021: AFD

V3 Vedecký výstup publikačnej činnosti z časopisu

V3_01 FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam. Simple power analysis attack on the QC-LDPC McEliece cryptosystem. In *Tatra Mountains Mathematical Publications*. Vol. 67, (2016), s. 85-92. ISSN 1210-3195 (2016: 0.367 - SJR, Q3 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85014730719.
Kategória publikácie do 2021: ADN
Ohlasy:
1. [1] BALDI, Marco - BARENGHI, Alessandro - CHIARALUCE, Franco - PELOSI, Gerardo - SANTINI, Paolo. LEDAkem: A post-quantum key encapsulation mechanism based on QC-LDPC Codes. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018-01-01, 10786 LNCS, pp. 3-24. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
2. [1] GUO, Ying - OU, Yu - LI, Lang. Construction of a high efficient distinguisher in differential power analysis attacks. In Proceedings of Science, 2017-01-01, 2017-December, pp., Registrované v: SCOPUS
Ohlas: zahraničný
3. [1] SANTINI, Paolo - BATTAGLIONI, Massimo - CHIARALUCE, Franco - BALDI, Marco. Analysis of reaction and timing attacks against

cryptosystems based on sparse parity-check codes. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019-01-01, 11666 LNCS, pp. 115-136. ISSN 03029743., Registrované v: SCOPUS
Ohlas: zahraničný
4. [1] SIM, Bo Yeon - HAN, Dong Guk. A study on the side-channel analysis trends for application to IoT devices. In Journal of Internet Services and Information Security, 2020-02-01, 10, 1, pp. 2-21. ISSN 21822069., Registrované v: SCOPUS
Ohlas: zahraničný
5. [1] SANTINI, Paolo - BALDI, Marco - CHIARALUCE, Franco. Complexity of statistical attacks on QC-LDPC code-based cryptosystems. In IET Information Security, 2020-05-01, 14, 3, pp. 304-312. ISSN 17518709., Registrované v: SCOPUS
Ohlas: zahraničný
6. [1] CHOWDHURY, Sreeja - COVIC, Ana - ACHARYA, Rabin Yu - DUPEE, Spencer - GANJI, Fatemeh - FORTE, Domenic. Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions. In Journal of Cryptographic Engineering, 2021-01-01, pp. ISSN 21908508., Registrované v: SCOPUS
Ohlas: zahraničný
7. [1] CAO, Yuan - LU, Xu - WU, Yanze - XIE, Haodong - QIAO, Yunkai - YAO, Enyi - CHEN, Shuai - YE, Jing. The Survey of Post-quantum Cryptography Hardware Implementation. In Journal of Cyber Security, 2021-11-01, 6, 6, pp. 1-16. ISSN 20961146., Registrované v: SCOPUS
Ohlas: zahraničný

V3_02 FABŠIČ, Tomáš - GROŠEK, Otokar - NEMOGA, Karol - ZAJAC, Pavol. On generating invertible circulant binary matrices with a prescribed number of ones. In *Cryptography and Communications*. Vol. 10, Iss. 1 (2018), s. 159-175. ISSN 1936-2447 (2018: 1.099 - IF, Q2 - JCR Best Q, 0.547 - SJR, Q2 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85041074817 ; CC: 000428746900011.
Kategória publikácie do 2021: ADC
Ohlasy:
1. [1] JITMAN, Somphong. Determinants of some special matrices over commutative finite chain rings. In SPECIAL MATRICES, 2020, vol. 8, no. 1, pp. 242-256. ISSN 2300-7451., Registrované v: WOS
Ohlas: zahraničný

V3_03 GROŠEK, Otokar - FABŠIČ, Tomáš. Computing multiplicative inverses in finite fields by long division. In *Journal of Electrical Engineering*. Vol. 69, No. 5 (2018), s. 400-402. ISSN 1335-3632 (2018: 0.636 - IF, Q4 - JCR Best Q, 0.200 - SJR, Q3 - SJR Best Q). V databáze: WOS: 000453413200012 ;

SCOPUS: 2-s2.0-85059569379.
Kategória publikácie do 2021: ADN

V3_04 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 (2019: 0.432 - IF, Q3 - JCR Best Q, 0.106 - SJR, Q4 - SJR Best Q). V databáze: CC: 000469567400001 ; DOI: 10.1080/01611194.2019.1596997.
Kategória publikácie do 2021: ADC
Ohlasy:
1. [1] FADLAN, Muhammad - HARYANSYAH - ROSMINI. Three Layer Encryption Protocol: an Approach of Super Encryption Algorithm. In 3rd International Conference on Cybernetics and Intelligent Systems (ICORIS 2021), 2021, pp. 267-271. ISBN 978-1-6654-2580-3., Registrované v: WOS, SCOPUS, IEEE
Ohlas: zahraničný
2. [2] FADLAN, Muhammad - HARYANSYAH - ROSMINI. Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom. In Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 2021, Vol. 5, no. 6, pp. 1113-1119. ISSN 2580-0760.
Ohlas: zahraničný
3. [2] Bauer, Craig P. Secret History: The Story of Cryptology, New York : Taylor & Francis Group, 2021. p. 640. ISBN 9781315162539.
Ohlas: zahraničný
4. [2] Muslih - Lekso Budi Handoko. Pengujian avalanche effect pada kriptografi teks menggunakan autokey cipher. In 2st Proceeding STEKOM 2022, 2022. Vol. 2 no. 1, pp. 127-134. ISSN 2809-1574
Ohlas: zahraničný

O2 Odborný výstup publikačnej činnosti ako časť knižnej publikácie alebo zborníka

O2_01 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.
Kategória publikácie do 2021: BFA

O2_02 FABŠIČ, Tomáš. A reaction attack on LEDApkc. In *CBC 2018 : The Sixth Code-Based Cryptography Workshop. Abstracts. Davie, Florida, USA. April 5-6, 2018*. Florida : Atlantic University, 2018, [1] s.
Kategória publikácie do 2021: BFA

I1 Iný výstup publikačnej činnosti ako celok

I1_01 FABŠIČ, Tomáš. *Contributions to the Analysis of the QC-LDPC McEliece Cryptosystem : dát. obhaj. 23.11.2017, č. ved. odboru 9-2-9*. 2017. 119 s. Dostupné na internete: <http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=130770>.
Kategória publikácie do 2021: DAI

I2 Iný výstup publikačnej činnosti ako časť publikácie alebo zborníka

I2_01 FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam. Demonstration of acoustic cryptanalysis. In *CryptArchi 2017 [elektronický zdroj] : 15th International workshop on cryptographic architectures embedded in logic devices. Smolenice, Slovakia. June 18-21, 2017*. Saint-Étienne : Laboratoire Hubert Curien, 2017, online, S. 11.
Kategória publikácie do 2021: GHG

I2_02 FABŠIČ, Tomáš - GALLO, Ondrej - GROŠEK, Otokar - HROMADA, Viliam - ZAJAC, Pavol. Post-quantum cryptography research at UIM FEI STU. In *Kvantové rendezvous : Smolenice. 29.6.-1.7.2022*, [5] s.
Typ výstupu: časti, ktoré nemožno zaradiť do kategórie V, O, P, U alebo D; Výstup: domáci; Kategória publikácie do 2021: GII

Počet doktorandov, ktorým je alebo bol školiteľom s určením, koľkí z nich štúdium ku dňu vyhotovenia životopisu riadne skončili: -

Názov študijného odboru, v ktorom bude uchádzač pôsobiť: **Informatika**

Počet uchádzačov: 1

- **1 pracovného miesta *odborného asistenta*** pre študijný odbor **Informatika** na Ústav informatiky a matematiky FEI STU od 1.6.2023 uspel:

Ing. Zuzana Rábeková

Zoznam členov výberovej komisie v rozsahu meno a priezvisko:

Martin Weis

Martin Drozda

Oľga Nánásiová

Milan Vojvoda

Danica Rosinová

Údaje vybraného uchádzača:

Meno, priezvisko, rodné priezvisko: Zuzana Rábeková, Bukovčíková

Akademické tituly, vedecko-pedagog. tituly, umelecko-pedagog. tituly, vedecké hodnosti:

Ing.

Rok narodenia: 1993

Údaje o vysokoškolskom vzdelaní, ďalšom akademickom raste a absolvovanom ďalšom vzdelávaní:

FEI STU v Bratislave - *Doktorandské štúdium*

SEPTEMBER 2017 - SÚČASNOSŤ (S PRERUŠENÍM SEPTEMBER 2021 - AUGUST 2023)

- Téma dizertačnej práce: Obsahovo orientované prehľadávanie obrazov pre biometriu

FEI STU v Bratislave - *Inžinierske štúdium*

SEPTEMBER 2015 - JÚN 2017

FEI STU v Bratislave - *Bakalárske štúdium*

SEPTEMBER 2012 - JÚN 2015

Údaje o priebehu zamestnaní a priebehu pedagogickej činnosti:

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE - Výskumný pracovník

JÚN 2021 - SÚČASNOSŤ

- Vykonávanie výskumnej činnosti v oblasti strojového učenia a počítačového videnia
- Pedagogická činnosť pozostávajúca z výučby a vedenia záverečných prác

NEW AGE FACTORY - Výskumný pracovník/Vývojár

OKTÓBER 2017 - DECEMBER 2021

PRACOVNÉ ZRUČNOSTI

- Výskumné a programátorské činnosti spojené s vývojom softvéru na indexovanie kolekcií pomocou Umelej inteligencie

- Skúsenosti s programovaním Machine Learning systémov a dátovou analýzou v programovacích jazykov Python a C++.

- Skúsenosti s trénovaním a evaluáciou modelov strojového učenia v oblastiach spracovania tabuľkových dát, obrazu a prirodzeného jazyka.

- Skúsenosti s vedením cvičení na II. stupni vysokolského štúdia (predmetov Strojové učenie a neurónové siete, Biometria a Artificial Intelligence and Data Processing) .

- Skúsenosti s vedením záverečných prác (12 bakalárskych prác a 12 diplomových prác).

Údaje o odbornom alebo umeleckom zameraní:

VÝSKUMNÉ AKTIVITY

Zodpovedný riešiteľ projektu:

- Artificial Intelligence in Medicine and Digital Cultures (AIMeDiC) – Interný FEI STU projekt na podporu mladých excelentnych tímov, 2022-2024

Spoluriešiteľ na prebiehajúcich projektoch:

- INOLab – Centrum pre inovácie a kybernetickú bezpečnosť, projekt aplikovaného výskumu FEI STU v Bratislave a NBS (Národná banka Slovenska) v oblastiach aplikácie umelej inteligencie, strojového učenia, matematických metód, kybernetickej bezpečnosti, 2020 –

- NITT SK II - Národná infraštruktúra pre podporu transferu technológií na Slovensku, 2016-2023

Spoluriešiteľ na ukončených projektoch:

- MLbiomedia – Advanced Machine Learning Methods for Proposal of Biometrics and Medical Diagnostic Systems, grant of the Slovak scientific grant agency VEGA 1/0867/17 (principal investigator M.Oravec, FEI STU), 2017-2020

Údaje o publikačnej činnosti:

Zoznam publikácii registrovaných v databázach Web of Science alebo Scopus:

[1] Andicsova, V., Bukovcikova, Z., Sopiak, D., Oravec, M., Automatic Recognition of Native Advertisements for the Slovak Language (2022) Communications in Computer and Information Science, 1527 CCIS, pp. 161-171. Cited 1 time.

DOI: 10.1007/978-3-030-96878-6_15

[2] Gajdos, M., Bukovcikova, Z., Sopiak, D., Oravec, M., Dataset Modification Captured in Uncontrolled Conditions (2020) Proceedings Elmar - International Symposium Electronics in Marine, 2020-September, art. no. 9219042, pp. 129-132.

DOI: 10.1109/ELMAR49956.2020.9219042

[3] Vizvary, L., Sopiak, D., Oravec, M., Bukovcikova, Z., Image quality detection using the siamese convolutional neural network (2019) Proceedings Elmar - International Symposium Electronics in Marine, 2019-September, art. no. 8918678, pp. 109-112. Cited 2 times.

DOI: 10.1109/ELMAR.2019.8918678

[4] Sopiak, D., Bukovčiková, Z., Oravec, M., Pavlovičová, J., The analysis of quality indicators on face recognition in video frames (2018) Proceedings Elmar - International Symposium Electronics in Marine, 2018-September, art. no. 8534652, pp. 155-158.

DOI: 10.23919/ELMAR.2018.8534652

[5] Bukovcikova, Z., Sopiak, D., Oravec, M., Pavlovicova, J., Face verification using convolutional neural networks with Siamese architecture (2017) Proceedings Elmar - International Symposium Electronics in Marine, 2017-September, art. no. 8124469, pp. 205-208. Cited 14 times.

DOI: 10.23919/ELMAR.2017.8124469

[6] Sopiak, D., Oravec, M., Pavlovicova, J., Bukovcikova, Z., Dittingerova, M., Bilanska, A., Novotna, M., Gontkovic, J., Generating face images based on 3D morphable model (2016) 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, ICNC-FSKD 2016, art. no. 7603151, pp. 58-62. Cited 1 time.

DOI: 10.1109/FSKD.2016.7603151

Celkový prehľad publikačnej činnosti:

Počet výstupov registrovaných v databázach Web of Science alebo Scopus	6
Počet citácii registrovaných v databázach Web of Science alebo Scopus	18

Ohlasy na vedeckú alebo umeleckú prácu: -

Počet doktorandov, ktorým je alebo bol školiteľom s určením, koľkí z nich štúdium ku dňu vyhotovenia životopisu riadne skončili: -

Názov študijného odboru, v ktorom bude uchádzač pôsobiť: **Informatika**

Počet uchádzačov: 1

- **1 pracovného miesta *odborného asistenta*** pre študijný odbor **Informatika** na Ústav informatiky a matematiky FEI STU od 1.7.2023 neuspel:

Ing. Maroš Baumgartner

Zoznam členov výberovej komisie v rozsahu meno a priezvisko:

Martin Weis

Martin Drozda

Oľga Nánásiová

Milan Vojvoda

Danica Rosinová

Údaje uchádzača:

Meno, priezvisko, rodné priezvisko: Maroš Baumgartner, Baumgartner

Akademické tituly, vedecko-pedagog. tituly, umelecko-pedagog. tituly, vedecké hodnosti:

Ing.

Rok narodenia: 1995

Údaje o vysokoškolskom vzdelaní, ďalšom akademickom raste a absolvovanom ďalšom vzdelávaní:

Od - do 09.2020 – (predpokladané ukončenie štúdia 08.2023)

Názov získanej kvalifikácie Doktorandské štúdium

Hlavné predmety / profesijné zručnosti Informatika

Názov a typ organizácie poskytujúcej vzdelávanie a prípravu: Fakulta elektrotechniky a informatiky, Technický univerzita v Košiciach, Letná 9, 040 01 Košice

Stupeň vzdelania v národnej alebo medzinárodnej klasifikácii: 3. Stupeň (Phylosophie doctor – PhD.)

Od- do 09.2018 – 06. 2020

Názov získanej kvalifikácie: Inžinierske štúdium

Hlavné predmety / profesíjne zručnosti: Informatika

Názov a typ organizácie poskytujúcej vzdelávanie a prípravu: Fakulta elektrotechniky a informatiky, Technický univerzita v Košiciach, Letná 9, 040 01 Košice

Stupeň vzdelania v národnej alebo medzinárodnej klasifikácii: 2. Stupeň (Engineer – Ing.)

Od – do 09.2015 – 06.2018

Názov získanej klasifikácie: Bakalárske štúdium

Hlavné predmety / profesíjne zručnosti: Telekomunikácie

Názov a typ organizácie poskytujúcej vzdelanie a prípravu: Fakulta elektrotechniky a informatiky, Technický univerzita v Košiciach, Letná 9, 040 01 Košice

Stupeň vzdelania v národnej alebo medzinárodnej klasifikácii: 1.stupeň (Bachelor – Bc.)

Od – do 2011 – 2015

Názov a typ organizácie poskytujúcej vzdelanie a prípravu: Stredná priemyselná škola, 069 01 Snina

Stupeň vzdelania v národnej alebo medzinárodnej klasifikácii: Úplné stredoškolské vzdelania s maturitou (elektrotechnik)

Údaje o priebehu zamestnaní a priebehu pedagogickej činnosti:

Od - do 09.2020 –

Zamestnanie alebo pracovné zaradenie: Quality Engineer

Hlavné činnosti a zodpovednosť: Testovanie webového a mobilného softvéru

Názov a adresa zamestnávateľa: Slovensko IT a.s., Štúrová 27, 040 01 Košice

Od - do 11.2021 – práve tu pracujem

Zamestnanie alebo pracovné zaradenie: Učiteľ fyziky a informatiky

Názov a adresa zamestnávateľa: Súkromná spojená škola, Starozágorská 8, 040 23 Košice

Od – do 2019 – 2020

Zamestnanie alebo pracovné zaradenie: Quality Engineer

Názov a adresa zamestnávateľa: Wirecard Slovakia s.r.o, Štúrová 27, 040 01 Košice

Od- do 2018 – 2019

Zamestnanie alebo pracovné zaradenie: Skladník

Názov a adresa zamestnávateľa: Heineken Slovensko, Južná trieda, Košice

Od – do 2016 – 2016

Zamestnanie alebo pracovné zaradenie: Pomocný elektrotechnik

Názov a adresa zamestnávateľa: UEZ s.r.o, Humenné

Od – do 2013 – 2015

Zamestnanie alebo pracovné zaradenie: Pomocný elektrotechnik

Názov a adresa zamestnávateľa: Stavbau group s.r.o, Česká republika

Údaje o odbornom alebo umeleckom zameraní: -

Údaje o publikačnej činnosti:

[1]. M. BAUMGARTNER, J. PAPAJ, N. KURKINA, L. DOBOS, "Game Theory and Decentralized Blockchain Technology Enabled for Secure and Reliable Routing in MANETs in 6G Environments", 2023 33nd International Conference Radioelektronika (RADIOELEKTRONIKA), Pardubice, Czech Republic, 2023. In press

[2]. N. KURKINA, J. PAPAJ, M. BAUMGARTNER, A. CIZMAR, "A new Approach for Routing in Cloud MANET", 2023 33nd International Conference Radioelektronika (RADIOELEKTRONIKA), Pardubice, Czech Republic, 2023. In press

[3]. M. BAUMGARTNER, 2023. ”Robust Data Transmission in 5G Networks Without Infrastructure”. 23st Scientific Conference of Young Researchers, 2023.

[4]. M. BAUMGARTNER, 2022. ”Use of blockchain technology in the routing process for multi-hop networks”. 22st Scientific Conference of Young Researchers, 2022.

[5]. M. BAUMGARTNER, J. PAPAJ, "Robust Data Transmission in 5G Networks Without Infrastructure Based on Blockchain Technology," 2022 32nd International Conference Radioelektronika (RADIOELEKTRONIKA), Kosice, Slovakia, 2022, pp. 01-04, doi: 10.1109/RADIOELEKTRONIKA54537.2022.9764944.

[6]. M. BAUMGARTNER, N. KURKINA, J. PAPAJ, R. NEZNIK, “Secure routing in 6G network”, 2022. Electrical Engineering and Informatics XIII (EEI), 2022.

[7]. N. KURKINA, M. BAUMGARTNER, J. PAPAJ, “Problematika smerovania v Cloud MANET”, 2022. Electrical Engineering and Informatics XIII (EEI), 2022.

[8]. M. BAUMGARTNER, N. KURKINA, J. PAPAJ, “Robustný Prenos Dát v 5G Sieťach bez Infraštruktúry Založený na Technológii Blockchain”, 2022. Electrical Engineering and Informatics XIII (EEI), 2022.

[9]. M. BAUMGARTNER, J. PAPAJ, E. ŠARŠALA, “Model D2D Komunikácie pre 5G Siete”, 2022. Electrical Engineering and Informatics XIII (EEI), 2022.

[10]. G. VAŠKOVÁ, N. KURKINA, M. BAUMGARTNER, J. PAPAJ, “Alternatívne metódy smerovania pre 6G siete”, 2022. Electrical Engineering and Informatics XIII (EEI), 2022.

[11]. M. BAUMGARTNER, J. JUHAR, J. PAPAJ, 2021. Short Performance Analysis of the LTE and 5G Access Technologies in NS-3, 16th Conference on Computer Science and Intelligence Systems, FedCSIS, 2021.

[12]. M. BAUMGARTNER, 2021. Robust data transmission in 5g networks without infrastructure. 21st Scientific Conference of Young Researchers, 2021.

[13]. M. BAUMGARTNER, J. JUHAR, J. PAPAJ, 2021. Simulation of 5G and LTE-Access Technologies Via Network Simulator NS-3. 44th International Conference on Telecommunications and Signal Processing (TSP), 2021.

[14]. M. BAUMGARTNER, J. JUHAR, J. PAPAJ, 2021. Simulovanie LTE a 5G prístupových technológií z pohľadu energetickej účinnosti s využitím NS-3. Electrical Engineering and Informatics XII (EEI), 2021.

[15]. M. BAUMGARTNER, J. JUHAR, J. PAPAJ, 2021. Výkonová analýza prístupových technológií 5G sietí v simulátore NS-3. Electrical Engineering and Informatics XII (EEI), 2021.

[16]. Návrh ad-hoc Siete pre Prenos Videotokov z Nepilotovaných Lietajúcich Prostriedkov. Electrical Engineering and Informatics 11. 2020. ISBN 978-80-553-3585-8.

[17]. M. BAUMGARTNER, J. JUHAR, J. PAPAJ, 2021. Performance and Efficiency Analysis of LTE-A and 5G Access Technologies Via NS-3. Acta Electronica et Informatica (AEI), 2021. ISSN 1338-395

Ohlasy na vedeckú alebo umeleckú prácu: -

Počet doktorandov, ktorým je alebo bol školiteľom s určením, koľkí z nich štúdium ku dňu vyhotovenia životopisu riadne skončili: -

Počet uchádzačov: 2

- **1 pracovného miesta *odborného asistenta*** pre študijný odbor **Informatika** na Ústav informatiky a matematiky FEI STU od 1.7.2023 uspel:

Mgr. Jozef Kollár, PhD.

Zoznam členov výberovej komisie v rozsahu meno a priezvisko:

Martin Weis

Martin Drozda

Oľga Nánásiová

Milan Vojvoda

Danica Rosinová

Údaje vybraného uchádzača:

Meno, priezvisko, rodné priezvisko: Jozef Kollár, Kollár

Akademické tituly, vedecko-pedagog. tituly, umelecko-pedagog. tituly, vedecké hodnosti:

Mgr., PhD.

Rok narodenia: 1968

Údaje o vysokoškolskom vzdelaní, ďalšom akademickom raste a absolvovanom ďalšom vzdelávaní:

2018 Ukončenie DPŠ v obore „Matematika“ na pedagogickej fakulte Trnavskej univerzity.

2016 PhD v odbore „Aplikovaná informatika“ na FEI STU v Bratislave, titul PhD.

1992 Diplom z matematiky a teoretickej informatiky na Matematicko Fyzikálnej Fakulte

UK v Bratislave, titul Mgr.

1991 Posledný semester štúdia absolvovaný na UNI Bremen, absolvovanie PNDS skúšky

1986–1992 Štúdium matematiky na MFF UK v Bratislave

1986 Maturita na strednej priemyselnej škole elektrotechnickej, Zochova 9, Bratislava

Údaje o priebehu zamestnaní a priebehu pedagogickej činnosti:

1992– . . . Vedecko-výskumný pracovník na Slovenskej Technickej Univerzite v Bratislave /

Katedra matematiky a deskriptívnej geometrie, SvF / Oddelenie matematiky, ÚIM

FEI / externista FIIT

Pracovné činnosti:

Výuka matematiky na stavebnej fakulte (SvF), fakulte elektrotechniky (FEI), fakulte informatiky (FIIT) a fakulte architektúry (FA)

Výuka informatiky

Výuka matematiky v prípravných kurzoch na príjimacie pohovory na SvF STU

Organizácia a príprava prípravných kurzov na príjimacie pohovory na SvF STU

Pedagóg zodpovedný za zostavovanie testov na príjimacie pohovory z matematiky pre

SvF STU

Budovanie a správa počítačovej siete Katedry matematiky na SvF STU

Správca servrov Katedry matematiky na SvF STU

1993–2002 Čiastočný úväzok ako učiteľ na Fakulte Managementu Univerzity Komenského

v Bratislave /

Pracovné činnosti:

Výuka matematiky

Výuka matematického softvéru (Wolfram Mathematica)

1998–2013 Pedagóg zodpovedný za zostavovanie prijímacích pohovorov z matematiky pre

Fakultu Managementu Univerzity Komenského v Bratislave

V rokoch 2004–2013 ako jediný autor a zostavovateľ úloh

Výuka matematiky v prípravných kurzoch na príjimacie pohovory pre FM UK

Organizácia a príprava prípravných kurzov na príjimacie pohovory pre FM UK

Matematicko pedagogické aktivity

1986–1995 Vedúci matematického krúžku pre talentované deti (veková kategória 13–18 rokov)

1988–1995 Organizácia a vedenie matematických prázdninových táborov a sústredení pre

rôzne matematické súťaže (BKMS, matematická olympiáda)

1993–1994 Predseda bratislavského krajského výboru matematickej olympiády

1991–2023 Autor viacerých skrípt, zbierok a učebníc pre vysokoškolských študentov (FEI

STU, FIIT STU, SvF STU, FM UK) a študentov gymnázií (zbierky k prijímacím pohovorom)

Údaje o odbornom alebo umeleckom zameraní: -

Údaje o publikačnej činnosti:

Práce v kategórii A

• Emmanuel Faure, Thierry Savy, Barbara Rizzi1, Camilo Melani1, Oľga Stašová, Dimitri Fabr`eges, Róbert Špir, Mark Hammons, Róbert Čunderlík, Ga¨elle Recher, Benoˆıt Lombardot, Louise Duloquin, Ingrid Colin, Jozef Kollár, Sophie Desnoulez, Pierre Affaticati, Benoˆıt Maury, Adeline Boyreau, Jean-Yves Nief, Pascal Calvat, Philippe Vernier, Monique Frain, Georges Lutfalla, Yannick Kergosien, Pierre Suret, Mariana Remešíková, René Doursat, Alessandro Sarti, Karol Mikula, Nadine Peyriéras & Paul Bourgine, A workflow to process 3D+time microscopy images of developing organisms and reconstruct their cell lineage, Nature Communications 7, Article number: 8674

Práce v kategórii B

• Kollár Jozef, Soviet VIC Cipher: No Respector of Kerckhoff ’s Principles, Cryptologia 40, 2015/2016, s. 33-48.

Práce v zahraničných nekarentovaných časopisoch

1. Kollár Jozef, Tajné písmo Martina Kukučína, Crypto-World, ISSN 1801-2140, Roč. 12, č. 1 (2010), s. 12–16

2. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny Úvod k seriálu, Crypto-World, ISSN 1801-2140, Roč. 13, č. 1 (2011), s. 2

3. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny Diel 1.: Šifra TTS, Crypto-World, ISSN 1801-2140, Roč. 13, č. 1 (2011), s. 3–11

4. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny Diel 2.: Šifra „Rímska dvaÿ, Crypto-World, ISSN 1801-2140, Roč. 13, č. 2 (2011), s. 2–11

5. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny Diel 3.: Šifra „Rímska osemÿ, Crypto-World, ISSN 1801-2140, Roč. 13, č. 3 (2011), s. 2–12

6. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny Diel 4.: Šifra „Rímska deväťÿ, Crypto-World, ISSN 1801-2140, Roč. 13, č. 4 (2011), s. 2–16

7. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny Diel 5.: Šifra „Rímska desaťÿ, Crypto-World, ISSN 1801-2140, Roč. 13, č. 5 (2011), s. 2–13

8. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny Diel 6.: Šifra „Rímska trinásťÿ, Crypto-World, ISSN 1801-2140, Roč. 13, č. 6 (2011), s. 2–11

9. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny Diel 7.: Šifra „Evaÿ, Crypto-World, ISSN 1801-2140, Roč. 13, č. 7-8 (2011), s. 2–9

10. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny Diel 8.: Šifra „Martaÿ, Crypto-World, ISSN 1801-2140, Roč. 13, č. 9 (2011), s. 2–8

11. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny. Diel 9., Šifra „Růženaÿ, Crypto-World, ISSN 1801-2140, Roč. 13, č.10 (2011), s. 2–12

12. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny. Diel 10., Šifra „Utilityÿ, Crypto-World, ISSN 1801-2140, Roč. 14, č. 2 (2012), s. 2–10

13. Kollár Jozef, ČS Šifry z obdobia 2. svetovej vojny. Diel 11., Šifra „Palackýÿ, Crypto-World, ISSN 1801-2140, Roč. 14, č. 3-4 (2012), s. 2–12

14. Kollár Jozef, Má zmysel používať autokľúč?, Crypto-World, ISSN 1801-2140, Roč. 14, č. 3-4 (2012), s. 12–17

15. Kollár Jozef, Andreas Figl – rakúsky dôstojník a kryptológ, Crypto-World, ISSN 1801-2140, Roč. 15, č. 3-4 (2013), s.15–23

16. Kollár Jozef, Häyhänen – sovietsky špión, Crypto-World, ISSN 1801-2140, Roč. 15, č. 7-8 (2013), s. 2–9

17. Kollár Jozef, Sovietska šifra VIC, Crypto-World, ISSN 1801- 2140, Roč. 15, č. 9-10 (2013), s. 2–16

Prezentácie na medzinárodných vedeckých konferenciách

1. Czechoslovak WWII Ciphers – pozvaná prednáška, Mikulášská kryptobesídka 2011: Sborník příspěvků, Praha 1.–2. decembra 2011, Praha: Trusted Network Solutions, 2011, s. 55–63

2. Czechoslovak WWII Ciphers Crypto History Experts Meeting, Heusenstamm, 7. jún 2012

3. Text reading direction of an unknown text, EuroHCC 2017, Smolenice, May 18th 2017

Prezentácie na domácich konferenciách

1. O písme Martina Kukučína, MAGIA 2009: Mathematics, Geometry and their Applications, Conference Proceedings, SvF STU v Bratislave, 2009, s. 149–152, ISBN 978-80-227-3207-9

2. Ako správne zvoliť heslo, MAGIA 2007: Mathematics, Geometry and their Applications, Conference Proceedings, SvF STU v Bratislave, 2007, s. 111–116

3. Centralizovaná správa hesiel, MAGIA 2007: Mathematics, Geometry and their Applications, Conference Proceedings, SvF STU v Bratislave, 2007, s. 117–125

4. Klasické transpozičné šifry, MAGIA 2006: Mathematics, Geometry and their Applications, Conference Proceedings, SvF STU, Bratislava 2006, s. 81–89, ISBN 80-227-2583-8
Matematika – tajná zbraň spojencov FMFI UK, Bratislava, (pozvaná prednáška), 13. september 2012

Skriptá a učebné texty

1. Kollár Jozef, Szökeová Danuše: Matematické úlohy z prijímacích skúšok, FM UK v Bratislave, 2016, ISBN 978-80-223-4094-6

2. Kollár Jozef, Matematika I. – Zbierka úloh ku cvičeniam, Bratislava: SvF STU, 2014, 167 s., ISBN 978-80-227-4244-3

3. Kollár Jozef, Riešené matematické úlohy z prijímacích skúšok FM UK 2008–2012, Bratislava: Univerzita Komenského v Bratislave, 2013, 383 s.

4. Kollár Jozef, Riešené matematické úlohy z prijímacích skúšok FM UK 2008–2011, Bratislava: Univerzita Komenského v Bratislave, 2012, 313 s., ISBN 978-80-223-3200-2

5. Kollár Jozef, Riešené matematické úlohy z prijímacích skúšok 2008–2009, Bratislava: Univerzita Komenského v Bratislave, 2010, 153 s., ISBN 978-80-223-2800-5

6. Kollár Jozef, Riešené matematické úlohy z prijímacích skúšok 2002–2007, Bratislava: Univerzita Komenského v Bratislave, 2008, 351 s., ISBN 978-80-223-2455-7

7. Kollár Jozef, Zbierka úloh z matematiky z prijímacích skúšok, Bratislava: FM UK v Bratislave, 2007., 264 s.

8. Kollár Jozef, Zbierka testov z matematiky na prijímacie skúšky, Bratislava: Univerzita Komenského v Bratislave, 2006

9. Kollár Jozef, Polakovič Marcel, Diskrétna matematika pre štundetov aplikovanej informatiky, Bratislava, Spectrum, FEI STU v Bratislave, 2020

Práca v riešiteľských kolektívoch

1.

Označenie: VEGA 1/0489/08

Názov: Topologické metódy štúdia diskrétnych štruktúr a ich grúp symetrií

Koordinátor: Prof. RNDr. Jozef Širáň, DrSc.

2.

Označenie: VEGA 1/0871/11

Názov: Algebraické a topologické metódy v štúdiu kombinatorických štruktúr s vysokým

stupňom súmernosti

Koordinátor: Prof. RNDr. Jozef Širáň, DrSc.

3.

Označenie: VEGA 1/3321/06

Názov: Moderné metódy matematického a počítačového modelovania v inžinierskych aplikáciách

Koordinátor: Prof. RNDr. Karol Mikula, DrSc.

4.

Označenie: VEGA 1/0269/09

Názov: Vývoj efektívnych a spoľahlivých numerických metód pre inžinierske aplikácie

Koordinátor: Prof. RNDr. Karol Mikula, DrSc.

5.

Označenie: Európsky projekt 6. rámcového programu Názov: EMBRYOMICS – Reconstructing in space and time the cell lineage tree (2005–2008)

Kontraktor: Prof. RNDr. Karol Mikula, DrSc.

Koordinátor: Dr. Nadine Peyrieras, CNRS Paris

6.

Označenie: Európsky projekt 6. rámcového programu

Názov: BioEmergencies: „In what" and „how much" are individuals similar and different? Towards the measurement of the individual susceptibility to diseases or response to treatments (2005–2009)

Kontraktor: Prof. RNDr. Karol Mikula, DrSc.

Koordinátor: Prof. P.Bourgine, Ecole Polytechnique, Paris

Ohlasy na vedeckú alebo umeleckú prácu: -

Počet doktorandov, ktorým je alebo bol školiteľom s určením, koľkí z nich štúdium ku dňu vyhotovenia životopisu: -

Názov študijného odboru, v ktorom bude uchádzač pôsobiť: **Informatika**

Počet uchádzačov: 2

V Bratislave, 27.04.2023

v. r. prof. Ing. Vladimír Kutiš, PhD.
d e k a n