



Záverečná karta projektu

Názov projektu

Evidenčné číslo projektu

APVV-19-0436

Nové informačné a komunikačné technológie pre budúcu informačnú infraštruktúru

Zodpovedný riešiteľ **prof. Ing. Peter Farkaš, DrSc.**

Príjemca

**Slovenská technická univerzita v Bratislave - Fakulta
elektrotechniky a informatiky**

Názov pracoviska, na ktorom bol projekt riešený

Názov: Slovenská technická univerzita v Bratislave

Adresa: Vazovova 5, 81243, Bratislava, Slovenská republika

IČO: 00397687

Názov a štát zahraničného pracoviska, ktoré spolupracovalo pri riešení

nedá sa aplikovať

Udelené patenty/podané patentové prihlášky, vynálezy alebo úžitkové vzory, ktoré sú výsledkami projektu

nedá sa aplikovať

Najvýznamnejšie publikácie (knihy, články, prednášky, správy a pod.) zhrňujúce výsledky projektu – uveďte aj publikácie prijaté do tlače

V1 Vedecký výstup publikačnej činnosti ako celok

V1_01 FARKAŠ, Peter. Linear Binary Block Codes Collection. 1. vydanie. Praha : Wolters Kluwer, 2024. 112 s. Dostupné na internete:

ISBN 978-80-7676-961-8.

Typ výstupu: monografia; Výstup: zahraničný; Kategória publikácie do 2021: AAA

V2 Vedecký výstup publikačnej činnosti ako časť editovanej knihy alebo zborníka

V2_01 FARKAŠ, Peter. Scalable family of codes with locality and availability for information repair in distributed storage systems. In Smart and Sustainable

Technologies : 4th International conference SpliTech 2019. Bol, Croatia. June 18-21, 2019.

1. vyd. Piscataway : IEEE, 2019, [USB-kľúč] Art. no. S13-

1570535407-1806. ISSN 978-953-290-091-0. V databáze: IEEE: 8783148 ; WOS: 000502810800030 ; SCOPUS: 2-s2.0-85070803296.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_02 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. V databáze: IEEE: 8806207 ; WOS:

000538761400007 ; SCOPUS: 2-s2.0-85072034350.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_03 FARKAŠ, Peter. Adaptive feedback supported communication for IoT and space applications. In AHS 2019 : NASA/ESA Conference on Adaptive Hardware and Systems. Colchester, UK. July 22-24, 2019. 1. vyd. Piscataway : IEEE Computer Society, 2019, S. 61-64. ISSN 2471-769X. ISBN 978-1-7281-4650-8. V databáze: DOI: 10.1109/AHS.2019.00005 ; SCOPUS: 2-s2.0-85071581007 ; IEEE: 8792938 ; WOS: 000494726000009.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_04 FARKAŠ, Peter - PÁLENÍK, Tomáš. On soft decoding of some binary RLL-transmission codes in systems with coherent BPSK modulation. In 2022 Cybernetics & Informatics (K&I) [elektronický zdroj] : Proceedings ; 31st International Conference; 11-14 September 2022 Visegrád, Maďarsko. 1. vydanie.

Danvers, Massachusetts, USA : IEEE, 2022, [5] s. ISBN 978-1-6654-8775-7. V databáze: DOI: 10.1109/KI55792.2022.9925949 ; SCOPUS: 2-s2.0-85142111124 ; IEEE: 9925949.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_05 PÁLENÍK, Tomáš - FARKAŠ, Peter - SCHINDLER, Frank. Accelerating weight spectrum calculation of linear block codes defined over GF(q) using GPU. In 2020 Cybernetics & Informatics (K&I) [elektronický zdroj] : 30th International Conference. Velké Karlovice, Czech Republic. January 29-February 1, 2020. 1.

ed. Danvers : IEEE, 2020, 140-145. ISBN 978-1-7281-4381-1. V databáze: IEEE: 9039806 ; SCOPUS: 2-s2.0-85083097601 ; WOS: 000753938900012 ; DOI: 10.1109/KI48306.2020.9039806.

Kategória publikácie do 2021: AFC

V2_06 RAKÚS, Martin - DIVINEC, Ladislav. A remote-access software-defined radio virtualized wireless communications laboratory. In IWSSIP 2021 : 28th International conference on systems, signals and image processing. Bratislava, Slovakia. June 2-4, 2021. 1. ed. Bratislava : Vydavateľstvo SPEKTRUM STU, 2021, S. 333-346. ISBN 978-80-227-5112-4.

Výstup: domáci; Kategória publikácie do 2021: AFD

V2_07 PÁLENÍK, Tomáš - SZITKEY, Viktor - OTRUBA, Jakub - DIVINEC, Ladislav. A minimal-resource

LDPC encoder and decoder design for memory-constrained systems. In ELEKTRO 2024 : 15th

International Conference. Zakopane, Poland. May 20-22, 2024. Danvers : IEEE, 2024, [6] s. ISBN 979-

8-3503-7234-2. V databáze: SCOPUS: 2-s2.0-85197397006.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC

V2_08 RALBOVSKÝ, Andrej - PÁLENÍK, Tomáš. Vulnerabilities of LTE and LTE-A Pro physical layer. 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.

Kategória publikácie do 2021: AFD

V2_09 RALBOVSKÝ, Andrej - PÁLENÍK, Tomáš. LTE physical layer security and resilience to DoS attacks.

In Redžúr 2019 : 13th International workshop on multimedia information and communication technologies. Bratislava, Slovakia. May 13, 2019. 1. vyd. Bratislava : Vydavateľstvo Spektrum STU,

2019, S. 11-14. ISBN 978-80-227-4931-2.

Kategória publikácie do 2021: AFD

V2_10 SZITKEY, Viktor - PÁLENÍK, Tomáš. Implementing a SDR communication system: simulations and

measurement. In ŠVOČ 2023 [elektronický zdroj] : Zborník vybraných prác. 26. apríl 2023. Bratislava :

Vydavateľstvo Spektrum STU, 2023, S. 15-20. ISBN 978-80-227-5307-4.

Typ výstupu: príspevok z podujatia; Výstup: domáci; Kategória publikácie do 2021: AFD

V2_11 FABŠIČ, Tomáš - GROŠEK, Otokar - HROMADA, Viliam - ZAJAC, Pavol. Post-Quantum Cryptography Migration: Challenges in Education. In Toward a Quantum-Safe

Communication Infrastructure : NATO Advanced Research Workshop. Valletta, Malta.
November 14-18, 2021. Amsterdam : IOS Press, 2024, S. 13-23. ISSN 1874-6268. ISBN
978-1-64368-498-7.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC
V3 Vedecký výstup publikačnej činnosti z časopisu

V3_01 FARKAŠ, Peter - RAKÚS, Martin - PÁLENÍK, Tomáš. A new technique for
incorporating RLL properties into 5G LDPC codes without additional redundancy.
In Wireless personal communications. Vol. 119, iss. 1(2021), s. 749-762. ISSN 0929-6212
(2021: 2.017 - IF, Q3 - JCR Best Q, 0.481 - SJR, Q2 - SJR Best Q).

V databáze: DOI: 10.1007/s11277-021-08235-3 ; WOS: 000619900100005 ; CC:
000619900100005 ; SCOPUS: 2-s2.0-85101215355.

Kategória publikácie do 2021: ADC

V3_02 FARKAŠ, Peter - RAKÚS, Martin. Decoding five times extended Reed Solomon
codes using syndromes. In Computing and Informatics. Vol. 39, no. 6 (2020),
s. 1311-1335. ISSN 1335-9150 (2020: 0.319 - IF, Q4 - JCR Best Q, 0.149 - SJR, Q4 - SJR
Best Q). V databáze: DOI: 10.31577/cai_2020_6_1311 ; WOS:
000654237200008 ; SCOPUS: 2-s2.0-85107847723 ; CC: 000654237200008.

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADD

V3_03 FARKAŠ, Peter - RAKÚS, Martin. On possible energy savings with transmission
supported via feedback channel in CubeSat transceiver. In Journal of
Electrical Engineering. Vol. 72, No. 5 (2021), s. 337-342. ISSN 1335-3632 (2021: 0.840 - IF,
Q4 - JCR Best Q, 0.200 - SJR, Q4 - SJR Best Q). V databáze:

DOI: 10.2478/jee-2021-0047 ; WOS: 000727374200007 ; SCOPUS: 2-s2.0-85141119781.

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADN

V3_04 FARKAŠ, Peter - DIVNEC, Ladislav - RAKÚS, Martin. Run length limited CCSDS
convolutional codes for optical communications. In Journal of Electrical
Engineering. Vol. 73, No. 6 (2022), s. 432-436. ISSN 1335-3632 (2022: 0.8 - IF, Q4 - JCR
Best Q, 0.218 - SJR, Q3 - SJR Best Q). V databáze: DOI:

10.2478/jee-2022-0059 ; WOS: 000903573600009 ; SCOPUS: 2-s2.0-85144935520.

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADN

V3_05 FARKAŠ, Peter - RAKÚS, Martin. Adding RLL properties to four CCSDS LDPC
codes without increasing their redundancy. In Computing and Informatics.
Vol. 42, no. 1 (2023), s. 157-197. ISSN 1335-9150 (2022: 0.7 - IF, Q4 - JCR Best Q, 0.196 -
SJR, Q4 - SJR Best Q). V databáze: DOI:

10.31577/cai_2023_1_157 ; WOS: 001014429100003 ; CC: 001014429100003 ; SCOPUS:
2-s2.0-85162841359.

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADD

V3_06 FARKAŠ, Peter. On adding security to RLL - LDPC CCSDS codes without additional
redundancy. In Journal of Electrical Engineering. Vol. 74, No. 3 (2023),
s. 184-187. ISSN 1335-3632 (2022: 0.8 - IF, Q4 - JCR Best Q, 0.218 - SJR, Q3 - SJR Best
Q). V databáze: DOI: 10.2478/jee-2023-0024 ; SCOPUS: 2-s2.0-
85166434512 ; WOS: 001034810000005.

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADN

V3_07 FARKAŠ, Peter - RAKÚS, Martin. Run Length Limited Error Control Codes Derived
from Reed Solomon Codes. In Wireless personal communications. Vol.
133, iss. 2 (2023), s. 795-810. ISSN 0929-6212 (2022: 2.2 - IF, Q3 - JCR Best Q, 0.545 -
SJR, Q2 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85180218514 ;
WOS: 001127093700004 ; DOI: 10.1007/s11277-023-10791-9.

Typ výstupu: článok; Výstup: zahraničný; Kategória publikácie do 2021: ADM

V3_08 FARKAŠ, Peter. Linear block code with locality and availability inspired by
tetrahedron. In Journal of Electrical Engineering. Vol. 75, No. 1 (2024), s. 72-76.
ISSN 1335-3632 (2022: 0.8 - IF, Q4 - JCR Best Q, 0.218 - SJR, Q3 - SJR Best Q). V
databáze: DOI: 10.2478/jee-2024-0010 ; WOS: 001161125900008 ;
SCOPUS: 2-s2.0-85187259601.

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADN

V3_09 FARKAŠ, Peter. Scalable codes with locality and availability derived from tessellation
via [7, 3, 4] Simplex code graph. In Journal of Electrical Engineering.
Vol. 75, No. 3 (2024), s. 192-197. ISSN 1335-3632 (2022: 0.8 - IF, Q4 - JCR Best Q, 0.218 -
SJR, Q3 - SJR Best Q). V databáze: DOI: 10.2478/jee-2024-0023

; SCOPUS: 2-s2.0-85196027060 ; WOS: 001241679500002.

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADN

V3_10 LACKO, Ján - RUŽICKÝ, Eugen - FARKAŠ, Peter. Faculty of informatics in Pan-european university in 2021 offers online seminaar to studets on trends in 5G and 6G. In Information Technology Applications. Vol. 9, No. 2 (2020), s. 3-10. ISSN 1338-6468.

Kategória publikácie do 2021: ADF

V3_11 RAKÚS, Martin - FARKAŠ, Peter - PÁLENÍK, Tomáš - DANIŠ, Andrej. Five times extended reed-solomon codes applicable in memory storage systems. In IEEE Letters of the Computer Society. Vol. 2, Iss. 2 (2019), s. 9-11. ISSN 2573-9689. V databáze: IEEE: 8691811.

Kategória publikácie do 2021: ADE

V3_12 RAKÚS, Martin - FARKAŠ, Peter - PÁLENÍK, Tomáš. Erasure decoding of five times extended Reed-Solomon codes. In Journal of Electrical Engineering. Vol. 70, No. 3 (2019), s. 256-258. ISSN 1335-3632 (2019: 0.686 - IF, Q4 - JCR Best Q, 0.204 - SJR, Q3 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85069678376 ; WOS: 000482659600010.

Kategória publikácie do 2021: ADN

V3_13 RAKÚS, Martin - FARKAŠ, Peter - PÁLENÍK, Tomáš. Modeling of mobile channels using TIMS in IT education. In Applied computing and informatics. Vol. 18, (2022), [15 s.]. ISSN 2634-1964 (2022: 0.932 - SJR, Q1 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85122062764 ; DOI: 10.1108/ACI-04-2021-0089.

Typ výstupu: článok; Výstup: zahraničný; Kategória publikácie do 2021: ADM

V3_14 PÁLENÍK, Tomáš - SZITKEY, Viktor. High throughput open-source implementation of Wi-Fi 6 and

WiMax LDPC encoder and decoder. In Information Technology Applications. Vol. 11, No. 2 (2022), s. 15-

32. ISSN 1338-6468. V databáze: DOI: 10.48550/arXiv.2306.12063.

V3_15 FARKAŠ, Peter. Faculty of informatics in Pan-european university in 2021 offers online seminaar to studets on trends in 5G and 6G. In Information Technology Applications. Vol. 13, No. 2 (2024), (v tlači) 1338-6468.

Kategória publikácie do 2021: ADF

V3_16 FARKAŠ, Peter - RAKÚS, Martin. New family of Linear 3-Erasure Correcting Block Codes over GF(q). In Computing and Informatics. Vol. 43, (2024), (v tlači). ISSN (2022: 0.7 - IF, Q4 - JCR Best Q, 0.196 - SJR, Q4 - SJR Best Q). V databáze: DOI: ; WOS: ; CC: ; SCOPUS:

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADD

P1 Pedagogický výstup publikačnej činnosti ako celok

P1_01 RAKÚS, Martin - PÁLENÍK, Tomáš. Digital communications – collection of solved problems and

examples. 1. ed. Camperdown : Emona Instruments, 2024. 246 s. ISBN 978-1-921903-15-1.

Typ výstupu: učebnica pre vysoké školy; Výstup: zahraničný; Kategória publikácie do 2021: ACA

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADF

O2 Odborný výstup publikačnej činnosti ako časť knižnej publikácie alebo zborníka

O2_01 TUČKOVÁ, Tamara - FABŠIČ, Tomáš. Investigating the resistance of REMP-1 and REMP-2 decoders against timing and syndrome attacks. In CECC 2024 : 24th Central European Conference on Cryptology. Warsaw, Poland. June 20-21, 2024. Warsaw : Military University of Technology, 2024, S. 42-45.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: BEE

O2_02 VAVRO, Tomáš - FABŠIČ, Tomáš. New decoders for QC-MDPC codes over GF(4). In CECC 2024 : 24th Central European Conference on Cryptology. Warsaw, Poland. June 20-21, 2024. Warsaw : Military University of Technology, 2024, S. 50-53.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: BEE

O2_03 BALÁŽ, Ján - COCHEROVÁ, Elena - FARKAŠ, Peter - FROLLO, Ivan - HAJDUKOVÁ, Mária - HARŤANSKÝ, René - KRAJČUŠKOVÁ, Zuzana -

ORSZÁGH, Juraj - ŠTOFANIK, Vladimír. URSI Slovak National Committee. In 100 years of the International Union of Radio Science. Gent : URSI Press,

Uplatnenie výsledkov projektu

Nakoľko sa jednalo o projekt základného výskumu jeho uplatnenie sa dá očakávať najmä v prispení k súčasnému a budúcemu stavu vedeckého poznania. V nasledujúcom zozname sú však uvedené aj oblasti možného uplatnenia v praxi v budúcej informačnej infraštruktúre IKT. Najvýznamnejšie uplatnenia výsledkov projektu k pokroku vo vedeckom poznaní a budúcej informačnej infraštruktúre IKT sú:

1. Navrhnutá technika prenosu s podporou v opačnom smere prenosu, ktorá umožňuje ušetriť energiu v uzloch, v ktorých je jej ohraničené množstvo na úkor energie centrálného uzla zberajúceho informáciu. Táto technika bola označená ako esenciálna pre masový výskum vesmíru v ohlase:

ARZO, S. T., et al. "Essential Technologies and Concepts for Massive Space Exploration: Challenges and Opportunities". In IEEE Transactions on aerospace and electronic systems. Vol. 59, Iss. 1 (2023), s. 3-29. ISSN 0018-9251., Registrované v: CC, WOS, SCOPUS (Ohlas: zahraničný)

Tento výsledok môže nájsť uplatnenie nielen v budúcej vesmírnej infraštruktúre IKT, ale aj v pozemnej infraštruktúre budúcich 6G mobilných sietí.

2. V monografii vydanej vo významnom zahraničnom vydavateľstve bolo publikovaných asi 200 najlepších lineárnych blokových kódov spolu s ich váhovými spektrami, ktoré v spojení s dekódovaním typu GRANT môžu prispieť k prekonaniu najväčšej prekážky pri vývoji komunikácii typ massive machine type communications (mMTC), a to súčasného zabezpečenia vysokej spoľahlivosti a nízkeho oneskorenia. mMTC bude tvoriť väčšinu objemu prenášanej užitočnej informácie v 6G. Tento výsledok môže nájsť uplatnenie nielen v budúcej vesmírnej infraštruktúre IKT, ale aj v budúcich systémoch IoT v 6G mobilných sieťach.

3. Konštruktívne sa podarilo dokázať že Reedove Solomonove kódy, ktoré sú v súčasnosti najvyužívanejšie v informačnej komunikačnej a pamäťovej infraštruktúre (v cloudoch) možno rozšíriť až 5x, pričom doterajšie poznanie uvádzalo, že to je možné urobiť len maximálne 3x. Pre takéto a príbuzné kódy boli v rámci projektu nájdene aj viaceré metódy ich kódovania a dekódovania. Tento výsledok môže nájsť uplatnenie nielen v budúcich úložiskách informácie pre jej uchovávanie, ktoré bude nevyhnutnou súčasťou budúcej pamäťovej IKT infraštruktúry.

4. Boli zostrojené nedvojkové kódy pre opravu troch zmazaní založené na kontrolnej matici zloženej z viacerých Vandermondových podmatic a premiešaných Vandermondových podmatic a bola navrhnutá metóda ich kódovania a dekódovania. Tento výsledok môže nájsť uplatnenie najmä v budúcich úložiskách informácie pre jej uchovávanie, ktoré bude nevyhnutnou súčasťou budúcej pamäťovej IKT infraštruktúry ale aj pri extrémne rýchlych prenosoch informácie optickými signálmi cez sklenené vlákna.

5. Bol zostrojený kód pre regeneráciu dát v distribuovaných dátových úložiskách s lokalitou 2 a viacnásobnou dostupnosťou 6 pre všetky uzly (servery) inšpirovaný štvorstenom a grafmi simplexného kódu. Tento kód okrem toho dosahuje hornú hranicu pre kódovú vzdialenosť. Tento výsledok môže nájsť uplatnenie nielen v budúcich úložiskách informácie pre jej uchovávanie, ktoré bude nevyhnutnou súčasťou budúcej pamäťovej IKT infraštruktúry.

6. Bola navrhnutá metóda pre zostrojenie nekonečnej množiny kódov pre regeneráciu dát v distribuovaných dátových úložiskách s lokalitou 2 a viacnásobnou dostupnosťou pre všetky uzly (servery) založená na "dláždení" roviny pomocou grafov simplexného kódu. Bola navrhnutá metóda ich dekódovania, ktorá umožňuje s veľkou pravdepodobnosťou regeneráciu stratenej informácie z uzlov zničených v rôznych oblastiach (napríklad zasiahnutých raketami a podobne). Metóda pripomína hojenie rán z niektorých biologických systémoch. Tento výsledok môže nájsť uplatnenie nielen v budúcich úložiskách informácie pre jej uchovávanie, ktoré bude nevyhnutnou súčasťou budúcej pamäťovej IKT infraštruktúry, a to pravdepodobne aj v prípade ničenia informačnej infraštruktúry teroristickými alebo vojnovými činnosťami.

7. Boli navrhnuté metódy pre konštrukcie dvoch nekonečných množín kódov pre regeneráciu dát v distribuovaných dátových úložiskách s lokalitou a viacnásobnou dostupnosťou pre všetky uzly (servery) založené na dvoj a troj- rozmerných fraktáloch.

Tento výsledok môže nájsť uplatnenie najmä v budúcich úložiskách informácie pre jej uchovávanie, ktoré bude nevyhnutnou súčasťou budúcej pamäťovej IKT infraštruktúry.

8. Bol zostrojený [36,12,12] kód násobok pre regeneráciu dát v distribuovaných dátových úložiskách s lokalitou a viacnásobnou dostupnosťou. Tento kód okrem toho dosahuje hornú hranicu pre kódovú vzdialenosť. Tento výsledok môže nájsť uplatnenie nielen v budúcich úložiskách informácie pre jej uchovávanie, ktoré bude nevyhnutnou súčasťou budúcej pamäťovej IKT infraštruktúry.

9. Bola navrhnutá metóda konštrukcie samoopravného kódu s obmedzenou jednosmernou zložkou v príslušnom linkovom signály typu BP NRZ. Tento výsledok môže nájsť uplatnenie v budúcej infraštruktúre IKT v sieťach typu IoT.

10. Boli navrhnuté metódy umožňujúce (pri typických okrajových podmienkach prenosu) dosiahnuť, aby niektoré CCSDS štandardizované LDPC kódy a CCSDS konvolučné kódy získali vlastnosti podporujúce synchronizáciu (RLL vlastnosti) bez vloženia ďalšej nadbytočnosti a zmeny metód dekódovania. Tento výsledok môže nájsť uplatnenie v budúcej vesmírnej infraštruktúre IKT.

11. Boli navrhnuté metódy umožňujúce bez vloženia ďalšej nadbytočnosti a zmeny metód dekódovania dosiahnuť aby štandardizované LDPC kódy pre 5G mobilné siete a nadobudli vlastnosti typu RLL podporujúce synchronizáciu. Tento výsledok môže nájsť uplatnenie v pozemnej infraštruktúre budúcich 5G mobilných sietí.

12. Bola navrhnutá metóda umožňujúca bez vloženia ďalšej nadbytočnosti a zmeny metód dekódovania (za splnenia istých okrajových podmienok prenosu) dosiahnuť, aby Reedove Solomonove kódy (RSC) zostrojené nad konečnými telesami charakteristiky 2 nadobudli vlastnosti typu RLL podporujúce synchronizáciu. Tento výsledok môže nájsť uplatnenie v pozemnej infraštruktúre IKT.

13. Boli navrhnuté dve metódy dekódovania QC-MDPC kódov zostrojených nad konečným poľom $GF(4)$ v systéme BIKE, ktorý je založený na McEliecevom post kvantovom kryptografickom systéme. Metódy sa vyznačujú podstatným zrýchlením procedúry dekódovania za cenu mierneho zhoršenia DFR. Tento výsledok môže nájsť uplatnenie v budúcej IKT infraštruktúre pri post kvantovej kryptografii. Systémy založené na McEliecevom kóde sa v súčasnosti zúčastňujú na 4. kole súťaže ktorú vyhlásil NIST v súvislosti so snahou o štandardizáciu budúcich post kvantových kryptografických systémov.

14. Boli navrhnuté 3 koncepcie ako generovať prídavné spoločné tajomstvo medzi komunikujúcimi stranami v hybridnom systéme zloženom z vonkajšieho Náhodného fontánového kódu a vnútorného McEliecevho kryptosystému. Tento výsledok môže nájsť uplatnenie v budúcej IKT infraštruktúre pri post kvantovej kryptografii. Systémy založené na McEliecevom kóde sa v súčasnosti zúčastňujú na súťaži, ktorú vyhlásil NIST v súvislosti so snahou o štandardizáciu budúcich post kvantových kryptografických systémov.

15. V zahraničnom vydavateľstva (v Austrálii) bola vydaná vysokoškolská učebnica obsahujúca zbierku vyriešených úloh v oblasti digitálnych komunikácií. Môže nájsť široké uplatnenie pri výučbe fyzickej vrstvy informačnej IKT infraštruktúry na univerzitách vo svete aj na Slovensku.

Okrem horeuvedených výsledkov základného výskumu boli realizované mnohé softvérové a iné produkty, inovované viaceré kurzy formálneho a neformálneho vzdelávania a iné, ktoré môžu byť uplatniteľné v praxi. Podrobnosti sú uvedené v ročných a záverečnej správe, kde sú aj opísané aplikačné výstupy.

Význam výsledkov môže dokresliť aj skutočnosť, že aj napriek tomu, že boli publikované len nedávno, existujú na ne nasledujúce citácie. U vedúceho projektu sa citácie na niektoré jeho publikácie dostávajú vo zvýšenej miere až po dvadsiatich rokoch, lebo značne predbiehajú poznanie v čase ich publikovania.

FARKAŠ, Peter. Scalable family of codes with locality and availability for information repair in distributed storage systems. In Smart and Sustainable Technologies : 4th International conference SpliTech 2019. Bol, Croatia. June 18-21, 2019. 1. vyd. Piscataway : IEEE, 2019, [USB-klúč] Art. no. S13-1570535407-1806. ISSN 978-953-290-091-0. V databáze: IEEE: 8783148 ; WOS: 000502810800030 ; SCOPUS: 2-s2.0-85070803296.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC Ohlas:

WANG, E. - WANG, Jing - LI, Jinghui - YANG, Jiarong. Construction of Optimal Locally Repairable Codes Based on Latin Square. In Beijing Youdian Xueyuan Xuebao. Vol. 46, iss. 5 (2023), s. 8-14. ISSN 1007-5321. V databáze: SCOPUS: 2-s2.0-85176113380 ; DOI:

10.13190/j.jbupt.2022-214 ; SCOPUS_INTID., Registrované v: SCOPUS

Ohlas: zahraničný

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. V databáze: IEEE: 8806207 ; WOS: 000538761400007 ; SCOPUS: 2-s2.0-85072034350.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC
Ohlas:

VAMBOL', Oleksij Sergijovič. Matematické metódy kryptoanalýzy a zvyšovanie produktivity asymetrických šifrov z špeciálnymi vlastnosťami. 1. vydanie. Kijev, Ukrajina : National Aerospace University "Kharkiv Aviation Institute", 2021. 153 s. Ohlas: zahraničný

FARKAŠ, Peter. Adaptive feedback supported communication for IoT and space applications. In AHS 2019 : NASA/ESA Conference on Adaptive Hardware and Systems. Colchester, UK. July 22-24, 2019. 1. vyd. Piscataway : IEEE Computer Society, 2019, S. 61-64. ISSN 2471-769X. ISBN 978-1-7281-4650-8. V databáze: DOI:

10.1109/AHS.2019.00005 ; SCOPUS: 2-s2.0-85071581007 ; IEEE: 8792938 ; WOS: 000494726000009.

Typ výstupu: príspevok z podujatia; Výstup: zahraničný; Kategória publikácie do 2021: AFC
Ohlasy:

1. [2] ARZO, Sisay Tadesse. Towards network automation: A multi-agent based intelligent networking system. 1. vydanie. Trento, Taliansko : University of Trento, 2021. 220 s.

Ohlas: zahraničný

2. [1] ARZO, Sisay Tadesse - SIKERIDIS, Dimitrios - DEVETSIKIOTIS, Michael - GRANELLI, Fabrizio - FIERRO, Rafael - ESMAELI, Mona - AKHAVAN, Zeinab. Essential Technologies and Concepts for Massive Space Exploration: Challenges and Opportunities. In IEEE transactions on aerospace and electronic systems. Vol. 59, Iss. 1 (2023), s. 3-29. ISSN 0018-9251 (4.400 - 2022). V databáze: WOS: 000948126100001 ; CC:

000948126100001 ; SCOPUS: 2-s2.0-85128640153., Registrované v: WOS, CC, SCOPUS

Ohlas: zahraničný

3. [1] ARZO, Sisay Tadesse - BASSOLI, Riccardo - DEVETSIKIOTIS, Michael - GRANELLI, Fabrizio - FITZEK, Frank H. P. Softwarization in Satellite and Interplanetary Networks. In Signals and Communication Technology [book series /]. 1. vydanie. Berlín, Nemecko : Springer Nature, 2023, S. 203-226. ISSN 1860-4862. V databáze: SCOPUS: 2-s2.0-85166159871., Registrované v: SCOPUS

Ohlas: zahraničný

FARKAŠ, Peter - RAKÚS, Martin - PÁLENÍK, Tomáš. A new technique for incorporating RLL properties into 5G LDPC codes without additional redundancy. In Wireless personal communications. Vol. 119, iss. 1(2021), s. 749-762. ISSN 0929-6212 (2021: 2.017 - IF, Q3 - JCR Best Q, 0.481 - SJR, Q2 - SJR Best Q). V databáze: DOI: 10.1007/s11277-021-08235-3 ; WOS: 000619900100005 ; CC: 000619900100005 ; SCOPUS: 2-s2.0-85101215355.

Kategória publikácie do 2021: ADC

Ohlasy:

1. [1] JIE, Zhang. Mobile Terminal Resource Sharing System for Network Ideological Guiding Considering Data Redundancy. In Proceedings of the Fifth International Conference on Electronics, Communication and Aerospace Technology : ICECA 2021. Piscataway, New York, USA : IEEE, 2021, S. 1727-1730. ISBN 978-1-6654-3524-6. V databáze: SCOPUS: 2-s2.0-85125393586 ; DOI: 10.1109/ICECA52323.2021.9675921., Registrované v: SCOPUS

Ohlas: zahraničný

V3_05 FARKAŠ, Peter - RAKÚS, Martin. Decoding five times extended Reed Solomon codes using syndromes. In Computing and Informatics. Vol. 39, no. 6 (2020), s. 1311-1335. ISSN 1335-9150 (2020: 0.319 - IF, Q4 - JCR Best Q, 0.149 - SJR, Q4 - SJR Best Q). V databáze: DOI: 10.31577/cai_2020_6_1311 ; WOS: 000654237200008 ; SCOPUS: 2-s2.0-85107847723 ; CC: 000654237200008.

Typ výstupu: článok; Výstup: domáci; Kategória publikácie do 2021: ADD

Ohlasy:

1. [1] PÁLENÍK, Tomáš - SZITKEY, Viktor - OTRUBA, Jakub - DIVINEC, Ladislav. A minimal-resource LDPC encoder and decoder design for memory-constrained systems. In ELEKTRO 2024 : 15th International Conference. Zakopane, Poland. May 20-22, 2024.

Danvers : IEEE, 2024, [6] s. ISBN 979-8-3503-7234-2. V databáze: SCOPUS: 2-s2.0-85197397006., Registrované v: SCOPUS

Ohlas: zahraničný

RAKÚS, Martin - FARKAŠ, Peter - PÁLENÍK, Tomáš. Erasure decoding of five times extended Reed-Solomon codes. In Journal of Electrical Engineering. Vol. 70, No. 3 (2019), s. 256-258. ISSN 1335-3632 (2019: 0.686 - IF, Q4 - JCR Best Q, 0.204 - SJR, Q3 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85069678376 ; WOS: 000482659600010.

Kategória publikácie do 2021: ADN

Ohlasy:

1. [1] SALAMA SARA - SALEM, Rashed - ABDEL-KADER, Hatem. Error detection and correction code using density-based clustering algorithm. In Proceedings ICCES 2019 - 14th International Conference on Computer Engineering and Systems : 17-18 December 2019, Cairo, Egypt. 1. vyd. New York, USA : IEEE, 2019, pp. 77-82. ISBN 978-1-7281-5260-8. V databáze: SCOPUS: 2-s2.0-85084704647., Registrované v: SCOPUS

Ohlas: zahraničný

V3_08 RAKÚS, Martin - FARKAŠ, Peter - PÁLENÍK, Tomáš. Modeling of mobile channels using TIMS in IT education. In Applied computing and informatics. Vol. 18, (2022), [15 s.]. ISSN 2634-1964 (2022: 0.932 - SJR, Q1 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85122062764 ; DOI: 10.1108/ACI-04-2021-0089.

Typ výstupu: článok; Výstup: zahraničný; Kategória publikácie do 2021: ADM

Ohlasy:

1. [1] THYAGATURU, Akhilesh S. - NGUYEN, Giang - RIMAL, Bhaskar Prasad - REISSLEIN, Martin. Ubi-Flex-Cloud: ubiquitous flexible cloud computing: status quo and research imperatives. In Applied computing and informatics, 2022, Vol. 18, [16 s.]. ISSN 2634-1964 (2022). V databáze: SCOPUS: 2-s2.0-85130516093., Registrované v: SCOPUS

Ohlas: zahraničný

2. [1] KLIUCHKA, Anatolii - HARTÁNSKÝ, René - HALGOŠ, Ján. Methods of computer modeling of electromagnetic field propagation in urban scenarios for Internet of Things. In Journal of Electrical Engineering. Vol. 74, No. 5 (2023), s. 422-433. ISSN 1335-3632. v databáze: WOS: 001098881700009 ; SCOPUS: 2-s2.0-85122062764, Registrované v: WOS, SCOPUS

Ohlas: domáci

3. [1] ALKHASAWNEH, Ruba - AL-NSOUR, Rawan - AKHO-ZAHIEH, Maryam. Measuring Online Engineering Laboratory Satisfaction During COVID-19 Pandemic. In Journal of Engineering Education Transformations. Vol. 37, iss. 3 (2024), s. 157-164. ISSN 2349-2473. V databáze: SCOPUS: 2-s2.0-85186872161 ; DOI: 10.16920/jeet/2024/v37i3/24011 ; SCOPUS_INTID., Registrované v: SCOPUS

Ohlas: zahraničný

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu v slovenskom jazyku (max. 20 riadkov)

Nasledujúci súhrn výsledkov projektu dokumentuje naplnenie cieľov projektu. Bola navrhnutá technika prenosu s podporou v opačnom smere, šetriaca energiu v uzloch s jej ohraničeným množstvom na úkor energie centrálného uzla. (V zahraničnom ohlase bola označená za esenciálnu pre masový výskum vesmíru.) Bolo zostrojených asi 200 najlepších lineárnych blokových kódov (LBC). Boli zostrojené najlepšie nedvojkové LBC, Konkrétne 4x a 5x rozšírené Reedove Solomonove kódy (RSC) a kód pre opravu 3 zmazaní. Boli zostrojené kódy pre regeneráciu dát s lokalitou a viacnásobnou dostupnosťou (LRCAC). Menovite [36,12,12] kód, [14,4,7] kód inšpirovaný štvorstenom, 2 nekonečné rodiny fraktálových LRCAC a 1 založená na dláždení roviny grafmi simplexného kódu. Boli navrhnuté metódy umožňujúce, aby niektoré štandardizované kódy získali RLL vlastnosti bez vloženia ďalšej nadbytočnosti a zmeny metód dekódovania. Jedná sa o CCSDS LDPC, CCSDS konvulčné kódy a 3GPP LDPC kódy pre 5G sieť. Takýto výsledok bol dosiahnutý aj pre RSC nad telesami rozšíreniami GF(2). Bola navrhnutá metóda konštrukcie LBC s obmedzenou jednosmernou zložkou v linkovom signále. Boli navrhnuté 2 rýchle metódy dekódovania QC-MDPC nad GF(4) pre post kvantové kryptosystémy typu McEliece. Boli navrhnuté 3 koncepcie generovania spoločného tajomstva v hybridnom kryptosystéme: Náhodný fontánový kód- McEliece. V zahraničí boli vydané 1 vysokoškolská učebnica a 1 monografia. Bolo publikovaných aj 11- V2, 16-V3 a 3-O2 publikácií. Výsledky sa môžu

uplatniť v budúcej informačnej IKT infraštruktúre. Sú to najmä pamäťové úložiská typu cloud, vesmírna a pozemská sieťová IKT infraštruktúra, IoT a post kvantová kryptografia.

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu v anglickom jazyku (max. 20 riadkov)

The following summary of the project results documents the achievement of the project's goals. A transmission technique with support in the reverse direction was proposed, which saves energy in nodes with limited amounts at the expense of the central node's energy. (In citation, it was described as essential for mass space research.) About 200 of the best linear block codes (LBC) were constructed. The best non-binary LBCs were also created, specifically 4x and 5x extendable Reed-Solomon codes (RSC) and a code for correcting 3 erasures. Codes for data regeneration with locality and multiple availability (LRCAC) were constructed. Notably, these include the $[36,12,12]$ code, the $[14,4,7]$ code inspired by the tetrahedron, 2 infinite families of fractal LRCACs, and one based on tiling the plane with simplex code graphs. Methods were devised to enable some standardized codes to acquire RLL properties without adding extra redundancy or changing decoding methods. These include CCSDS LDPC codes, CCSDS convolutional codes, and 3GPP LDPC codes for 5G networks. Such result was achieved also for RSC over $GF(2)$. A method for constructing LBC with a limited DC component in the corresponding line signal was proposed. Two fast methods for decoding QC-MDPC over $GF(4)$ in post-quantum cryptosystems (PQC) of the McEliece type were designed. Three concepts for generating a shared secret in a hybrid cryptosystem were proposed: Random fountain code-McEliece. Abroad, one university textbook and one monograph were published. Additionally, 11-V2, 16-V3, and 3-O2 publications were released. The results can be applied in future ICT infrastructure, especially cloud storage, space and terrestrial network ICT infrastructure, IoT, and PQC.