

Lista 10 articole reprezentative

Conferințe Internaționale

- 2021 **Structural properties of self-dual monomial codes with application to code-based cryptography**, *Vlad-Florin Drăgoi, Andreea Szocs*, 18th IMA International Conference on Cryptography and Coding IMACC, Dec. 2021, Virtual. (ISI WOS, Scopus).
https://doi.org/10.1007/978-3-030-92641-0_2
- 2021 **Message-Recovery laser fault injection attack on the Classic McEliece cryptosystem**, *Pierre-Louis Cayrel, Brice Colombier, Vlad-Florin Drăgoi, Alexandre Menu, Lilian Bossuet*, Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt), Oct. 2021, Zagreb, Croatia. (ISI WOS, Scopus).
https://doi.org/10.1007/978-3-030-77886-6_15
- 2016 **Algebraic Properties of Polar Codes From a New Polynomial Formalism**, *Magali Bardet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich*, IEEE International Symposium on Information Theory (ISIT), July 2016, Barcelona, Spain. (ISI WOS, Scopus).
<http://dx.doi.org/10.1109/ISIT.2016.7541295>
- 2016 **Weak Keys for the Quasi-Cyclic MDPC Public Key Encryption Scheme**, *Magali Bardet, Vlad Dragoi, Jean-Gabriel Luque, and Ayoub Otmani*, International Conference on Cryptology – AFRICACRYPT, April 2016, Fes, Morocco. (Scopus).
http://dx.doi.org/10.1007/978-3-319-31517-1_18
- 2016 **Cryptanalysis of the McEliece Public Key Cryptosystem based on Polar Codes**, *Magali Bardet, Julia Chaudet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich*, International Workshop on Post Quantum Cryptography (PQCrypt), Feb. 2016, Fukuoka, Japan. (ISI WOS, Scopus).
http://dx.doi.org/10.1007/978-3-319-29360-8_9

Reviste Internaționale

- 2021 **Fast reliability ranking of matchstick minimal networks**, *Vlad-Florin Dragoi, Valeriu Beiu*, Networks, early access, 2021. (ISI WOS, Scopus).
<https://doi.org/10.1002/net.22064>
- 2021 **Bhattacharyya parameter of monomial codes for the binary erasure channel :from point-wise to average reliability**, *Vlad-Florin Dragoi, Gabriela Cristescu*, Sensors, vol. 21, no. 9, 2021. (ISI WOS, Scopus).
<https://doi.org/10.3390/s21092976>
- 2021 **Efficient approximation of two-terminal networks reliability polynomials using cubic splines**, *Gabriela Cristescu, Vlad-Florin Dragoi*, IEEE Transactions on Reliability, vol. 70, no. 3, 2021. (ISI WOS, Scopus).
<https://doi.org/10.1109/TR.2021.3049957>
- 2020 **Studying the binary erasure polarization subchannels using network reliability**, *Vlad Drăgoi, Valeriu Beiu*, IEEE Communications Letters, vol.24, no.1, 2020. (ISI WOS, Scopus).
<http://doi.org/10.1109/LCOMM.2019.2947910>
- 2018 **Cryptanalysis of a Public Key Encryption Scheme Based on QC-LDPC and QC-MDPC**, *Vlad Dragoi, and Hervé Talé Kalachi*, IEEE Communications Letters, vol. 22, 2018. (ISI WOS, Scopus).
<http://doi.org/10.1109/LCOMM.2017.2779449>

Teza de doctorat

- 2017 **An algebraic approach for the resolution of algorithmic problems raised by cryptography and coding theory**, *Dragoi Vlad Florin*, Teză susținută în 06/07/2017, Universitatea din Rouen, Franța.
<https://tel.archives-ouvertes.fr/tel-01690012/file/dragoivladflorin2.pdf>

Articole publicate in Proceedings la Conferințe Internaționale

- 2021 **Structural properties of self-dual monomial codes with application to code-based cryptography**, *Vlad-Florin Drăgoi, Andreea Szocs*, 18th IMA International Conference on Cryptography and Coding IMACC, Dec. 2021, Virtual. (ISI WOS, Scopus).
https://doi.org/10.1007/978-3-030-92641-0_2
- 2021 **Message-Recovery laser fault injection attack on the Classic McEliece cryptosystem**, *Pierre-Louis Cayrel, Brice Colombier, Vlad-Florin Drăgoi, Alexandre Menu, Lilian Bossuet*, Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt), Oct. 2021, Zagreb, Croatia. (ISI WOS, Scopus).
https://doi.org/10.1007/978-3-030-77886-6_15
- 2020 **Why reliability for computing needs rethinking**, *Valeriu Beiu, Vlad-Florin Drăgoi, Roxana-Mariana Beiu*, International Conference on Rebooting Computing (IEEE-ICRC), Dec. 2020, Virtual. (ISI WOS, Scopus).
<https://doi.org/10.1109/ICRC2020.2020.00006>
- 2020 **Employing sorting nets for designing reliable computing nets**, *Mariana Nagy, Vlad-Florin Drăgoi, Valeriu Beiu*, International Conference on Nanotechnology (IEEE-NANO), July 2020, Virtual. (ISI WOS, Scopus).
<https://doi.org/10.1109/NANO47656.2020.9183395>
- 2020 **On recursively defined combinatorial classes and labelled trees**, *Ali Chouria, Vlad-Florin Drăgoi, Jean-Gabriel Luque*, International Conference on Computers Communications and Control, May 2020, Virtual. (ISI WOS, Scopus).
https://doi.org/10.1007/978-3-030-53651-0_2
- 2020 **Tight bounds on the coefficients of consecutive k-out-of-n :F systems**, *Vlad-Florin Drăgoi, Simon Cowell, Valeriu Beiu*, International Conference on Computers Communications and Control, May 2020, Virtual. (ISI WOS, Scopus).
https://doi.org/10.1007/978-3-030-53651-0_3
- 2018 **Vulnerabilities of the McEliece Variants Based on Polar Codes**, *Vlad Drăgoi, Valeriu Beiu, Dominic Bucerzan*, International Conference on Security for Information Technology and Communications (SecITC), November 8–9, 2018, Bucharest, Romania. (Scopus).
https://link.springer.com/chapter/10.1007/978-3-030-12942-2_29
- 2018 **On posets for reliability : How fine can they be?**, *Valeriu Beiu, Simon R. Cowell, Vlad-Florin Drăgoi*, International Workshop on Soft Computing Applications SOFA, Sept. 2018, Arad, Romania (Scopus).
https://doi.org/10.1007/978-3-030-51992-6_10
- 2018 **Effective Conductances of Moore-Shannon Hammocks**, *Simon R. Cowell, Vlad Drăgoi, Valeriu Beiu, Noemi Rohatinovici*, IEEE International Conference on Nanotechnology (IEEE-NANO), July 23-26, 2018, Cork, Ireland (ISI WOS).
<http://dx.doi.org/10.1109/NANO.2018.8626295>

- 2018 **Ordering Series and Parallel Compositions**, *Vlad Dragoi, Simon R. Cowell, Valeriu Beiu*, IEEE International Conference on Nanotechnology (IEEE-NANO), July 23-26, 2018, Cork, Ireland (ISI WOS).
<http://dx.doi.org/10.1109/NANO.2018.8626408>
- 2018 **Survey on Cryptanalysis of Code-Based Cryptography : From Theoretical to Physical Attacks**, *Vlad Dragoi, Tania Richmond, Dominic Bucerzan and Axel Legay*, IEEE International Conference on Computers Communications and Control, May 2018, Baile Felix, Oradea, Romania. (ISI WOS, Scopus).
<http://dx.doi.org/10.1109/ICCCC.2018.8390461>
- 2018 **Hammocks versus Hammock**, *Valeriu Beiu, Simon R. Cowell, Vlad Dragoi, Sorin Hoară and Păstorel Gașpar*, IEEE International Conference on Computers Communications and Control, May 2018, Baile Felix, Oradea, Romania. (ISI WOS, Scopus).
<http://dx.doi.org/10.1109/ICCCC.2018.8390447>
- 2018 **Can Series and Parallel Compositions Improve on Hammocks ?**, *Vlad Dragoi, Simon R. Cowell, Valeriu Beiu, Sorin Hoară and Păstorel Gașpar*, IEEE International Conference on Computers Communications and Control, May 2018, Baile Felix, Oradea, Romania. (ISI WOS, Scopus).
<http://dx.doi.org/10.1109/ICCCC.2018.8390448>
- 2018 **On Algorithms for Evaluating the Reliability of Large Hammock Networks**, *Noemi-Clara Rohatinovici, Valeriu Beiu, Simon R. Cowell, Leonard Daus, Vlad Dragoi and Valentina Emilia Balas*, IEEE International Conference on Computers Communications and Control, May 2018, Baile Felix, Oradea, Romania. (ISI WOS, Scopus).
<http://dx.doi.org/10.1109/ICCCC.2018.8390449>
- 2017 **The Simple Roots Problem**, *Dominic Bucerzan, Vlad Dragoi and Tania Richmond*, Romanian Cryptology Days (RCD), Sept. 18-20, 2017, Bucharest, Romania. (ISI WOS, Scopus).
<http://www.acad.ro/sectii2002/proceedings/doc2017-4s/03artSupl.pdf>
- 2017 **Evolution of the McEliece Public Key Encryption Scheme**, *Dominic Bucerzan, Vlad Dragoi and Hervé Talé Kalachi*, International Conference on Security for Information Technology and Communications (SeclTC), June 8-9, 2017, Bucharest, Romania. (Scopus).
https://link.springer.com/chapter/10.1007/978-3-319-69284-5_10
- 2016 **Algebraic Properties of Polar Codes From a New Polynomial Formalism**, *Magali Bardet, Vlad Dragoi, Ayoub Otmani, Jean-Pierre Tillich*, IEEE International Symposium on Information Theory (ISIT), July 10-15, 2016, Barcelona, Spain. (ISI WOS, Scopus).
<http://dx.doi.org/10.1109/ISIT.2016.7541295>
- 2016 **Weak Keys for the Quasi-Cyclic MDPC Public Key Encryption Scheme**, *Magali Bardet, Vlad Dragoi, Jean-Gabriel Luque, Ayoub Otmani*, Progress in Cryptology – AFRICACRYPT, April 13-15, 2016, Fes, Morocco. (Scopus).
http://dx.doi.org/10.1007/978-3-319-31517-1_18
- 2016 **Cryptanalysis of the McEliece Public Key Cryptosystem based on Polar Codes**, *Magali Bardet, Julia Chautet, Vlad Dragoi, Ayoub Otmani, Jean-Pierre Tillich*, International Workshop on Post Quantum Cryptography (PQCrypt), Feb. 24-26, 2016, Fukuoka, Japan. (ISI WOS, Scopus).
http://dx.doi.org/10.1007/978-3-319-29360-8_9

2015 **Etude d'un Système de Chiffrement de Type McEliece à Base de Codes Polaires**, *Magali Bardet, Julia Choulet, Vlad Dragoi, Ayoub Otmani, Jean-Pierre Tillich*, Journées Codage et Cryptographie, La Londe-les-Maures, França.

<https://hal.inria.fr/hal-01240843/>

2013 **Polynomial Structures in Code-based Cryptography**, *Vlad Dragoi, Pierre-Louis Cayrel, Brice Colombier, Tania Richmond*, 14th International Conference on Cryptology in India, Dec. 7-10, 2013, Mumbai, India. (Scopus).

http://dx.doi.org/10.1007/978-3-319-03515-4_19

Article publicate in Reviste Internationale

2021 **Generalized Convexity Properties and Shape-Based Approximation in Networks Reliability**, *Gabriela Cristescu, Vlad-Florin Dragoi, Sorin Horatiu Hoara*, Mathematics, vol. 9, no. 24, 2021. (ISI WOS, Scopus).

<https://doi.org/10.3390/math9243182>

2021 **Four Input Sorter Good, Larger Ones Not So Good**, *Vlad-Florin Dragoi, Simon Robin Cowell, Valeriu Beiu*, IEEE Transactions on Nanotechnology, vol. 20, 2021. (ISI WOS, Scopus).

<https://doi.org/10.1109/TNANO.2021.3113731>

2021 **Fast reliability ranking of matchstick minimal networks**, *Vlad-Florin Dragoi, Valeriu Beiu*, Networks, early access, 2021. (ISI WOS, Scopus).

<https://doi.org/10.1002/net.22064>

2021 **Bhattacharyya parameter of monomial codes for the binary erasure channel :from point-wise to average reliability**, *Vlad-Florin Dragoi, Gabriela Cristescu*, Sensors, vol. 21, no. 9, 2021. (ISI WOS, Scopus).

<https://doi.org/10.3390/s21092976>

2021 **Efficient approximation of two-terminal networks reliability polynomials using cubic splines**, *Gabriela Cristescu, Vlad-Florin Dragoi*, IEEE Transactions on Reliability, vol. 70, no. 3, 2021. (ISI WOS, Scopus).

<https://doi.org/10.1109/TR.2021.3049957>

2020 **Solving a Modified Syndrome Decoding Problem using Integer Programming**, *Vlad-Florin Dragoi, Pierre-Louis Cayrel, Brice Colombier, Dominic Bucerzan, Sorin Hoară*, International Journal of Computers Communications & Control, vol. 15, no. 5, 2020. (ISI WOS, Scopus).

<https://doi.org/10.15837/ijccc.2020.5.3920>

2020 **Studying the binary erasure polarization subchannels using network reliability**, *Vlad Drăgoi, Valeriu Beiu*, IEEE Communications Letters, vol.24, no.1, 2020. (ISI WOS, Scopus).

<http://doi.org/10.1109/LCOMM.2019.2947910>

2019 **Cubic Spline Approximation of the reliability polynomials of two dual hammock networks**, *Gabriela Cristescu, Vlad Drăgoi*, TJMM, vol.11, no.1-2, 2019.

<http://doi.org/10.1109/LCOMM.2019.2947910>

2018 **How Reliable are Compositions of Series and Parallel Networks Compared with Hammocks?**, *Vlad Dragoi, Simon R. Cowell, Valeriu Beiu, Sorin Hoară and Păstorel Gașpar*, International Journal of Computers Communications & Control, vol. 13, no. 5, 2018. (ISI WOS, Scopus).

<https://doi.org/10.15837/ijccc.2018.5.3354>

2018 **Cryptanalysis of a Public Key Encryption Scheme Based on QC-LDPC and QC-MDPC**, *Vlad Dragoi, Hervé Talé Kalachi* , IEEE Communications Letters, vol. 22 , 2018. (ISI WOS, Scopus).

<http://doi.org/10.1109/LCOMM.2017.2779449>

2017 **Improved Timing Attacks against the Secret Permutation in the McEliece PKC**, *Dominic Bucerzan, Pierre-Louis Cayrel, Vlad Dragoi, Tania Richmond*, International Journal of Computers Communications & Control , vol. 12, no. 1, 2017. (ISI WOS, Scopus).

<http://dx.doi.org/10.15837/ijccc.2017.1.2780>