PhD Thesis

2017 **An algebraic approach for the resolution of algorithmic problems raised by cryptography and coding theory**

https://tel.archives-ouvertes.fr/tel-01690012/file/dragoivladflorin2.pdf

International Conferences : Coding Theory and Cryptography

2026 **Algebraic Properties of PAC Codes**, *Vlad-Florin Drăgoi, Mohammad Rowshan*, 2026 IEEE International Symposium on Information Theory (ISIT), 28 June 2026 - 03 July 2026, Guangzhou, China .

https://doi.org/10.1109/ISIT62367.2026.11653640

2026 **Generalized Weight Structure of Polar Codes : Selected Template Polynomials**, *Vlad-Florin Drăgoi, Mohammad Rowshan*, 2026 IEEE International Symposium on Information Theory (ISIT), 28 June 2026 - 03 July 2026, Guangzhou, China .

https://doi.org/10.1109/ISIT62367.2026.11653734

2026 **Key-Recovery Side-Channel Attack on the Berlekamp-Massey Decoding Algorithm in the Classic McEliece KEM**, *Andrei Alexei, Marios Omar Choudary, Vlad-Florin Dragoi*, IACR Workshop on Cryptographic Hardware and Embedded Systems, CHES 2026.

https://ches.iacr.org/2026/acceptedpapers.php#issue4

2025 **Algebraic Key-Recovery Side-Channel Attack on Classic McEliece**, *Michaël Bulois, Pierre-Louis Cayrel, Vlad-Florin Drăgoi and Vincent Grosso*, Selected Areas in Cryptography (SAC) 2025, August 11–15, 2025 Toronto, Ontario.

https://sacworkshop.org/SAC25/preproceedings/sac2025-2-paper13.pdf

2025 **Full Key-Recovery Cubic-Time Template Attack on Classic McEliece Decapsulation**, *Vlad-Florin Drăgoi, Brice Colombier, Nicolas Vallet, Pierre-Louis Cayrel, Vincent Grosso*, IACR Transactions on Cryptographic Hardware and Embedded Systems, CHES 2025, 14-18 September, Kuala Lumpur, Malaysia.

https://doi.org/10.46586/tches.v2025.i1.367-391

2025 **Message-recovery Horizontal Correlation Attack on Classic McEliece**, *Brice Colombier, Vincent Grosso, Pierre-Louis Cayrel, Vlad-Florin Dragoi*, Conference on Constructive Approaches for Security Analysis and Design of Embedded Systems (CASCADE 2025), 2-4 Mars, Saint-Etienne, France.

https://doi.org/10.1007/978-3-032-01405-4_4

2025 **On Partial Weight Distribution of Polar Codes**, *Vlad-Florin Drăgoi, Mohammad Rowshan*, 2025 IEEE International Symposium on Information Theory (ISIT), 22-27 June 2025, Ann Arbor, Michigan, USA.

https://doi.org/10.1109/ISIT63088.2025.11195548

2025 **Towards Weight Distribution-Aware Polar Codes**, *Mohammad Rowshan, Vlad-Florin Drăgoi*, 2025 IEEE International Symposium on Information Theory (ISIT), 22-27 June 2025, Ann Arbor, Michigan, USA.

https://doi.org/10.1109/ISIT63088.2025.11195275

2024 **Weight structure of low/high-rate polar codes and its applications**, *Mohammad Rowshan, Vlad-Florin Drăgoi, Jinhong Yuan*, 2024 IEEE International Symposium on Information Theory (ISIT), 07-12 July 2024, Athens, Greece.

https://doi.org/10.1109/ISIT57864.2024.10619618

2023 **A Side-Channel Attack Against Classic McEliece When Loading the Goppa Polynomial**, *Boly Seck, Pierre-Louis Cayrel, Vlad-Florin Dragoi, Idy Diop, Morgan Barbier, Jean Belo Klamti, Brice Colombier, Vincent Grosso*, International Conference on Cryptology in Africa, Sousse, Tunisia, July 19–21, 2023.

https://doi.org/10.1007/978-3-031-37679-5_5

2023 **Punctured Syndrome Decoding Problem : Efficient Side-Channel Attacks Against Classic McEliece**, *Vlad-Florin Dragoi, Brice Colombier, Pierre-Louis Cayrel, Vincent Grosso*, International Workshop on Constructive Side-Channel Analysis and Secure Design COSADE 2023, April 3-4, Munich, Germany.

https://link.springer.com/chapter/10.1007/978-3-031-29497-6_9

2023 **Fast Methods for Ranking Synthetic BECs**, *Hsin-Po Wang, Vlad-Florin Dragoi*, IEEE International Symposium on Information Theory (ISIT), 25-30 June, Taipei, Taiwan, 2023.

https://ieeexplore.ieee.org/document/10206704

2022 **Key-Recovery by Side-Channel Information on the Matrix-Vector Product in Code-Based Cryptosystems**, *Boly Seck, Pierre-Louis Cayrel, Idy Diop, Vlad-Florin Dragoi, Kalen Couzon, Brice Colombier, Vincent Grosso*, International Conference, ICISC 2022, Seoul, South Korea, November 30 – December 2, 2022.

https://doi.org/10.1007/978-3-031-29371-9_11

2022 **Integer Syndrome Decoding Problem in the Presence of Noise**, *Vlad-Florin Dragoi, Brice Colombier, Pierre-Louis Cayrel, Vincent Grosso*, IEEE Information Theory Workshop (ITW), Nov. 6 - 9, Mumbai, India.

https://ieeexplore.ieee.org/abstract/document/9965806

2022 **Generalized Inverse based Decoding**, *Vlad-Florin Dragoi, Ferucio Laurentiu Tiplea*, IEEE International Symposium on Information Theory (ISIT), May 26 - June 1, 2022, Espoo, Finland.

https://doi.org/10.1109/ISIT50566.2022.9834696

2021 **Structural Properties of Self-Dual Monomial Codes with Applicationto Code-Based Cryptography**, *Vlad-Florin Drăgoi, Andreea Szocs*, 18th IMA International Conference on Cryptography and Coding IMACC, Dec. 2021, Virtual.

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.

https://doi.org/10.1007/978-3-030-77886-6_15

2020 **Combinatorial Algorithms for Integer Syndrome Decoding Problem**, *Vlad-Florin Dragoi, Alin Tiberiu Lacatus, Alexandru Popoviciu*, International Workshop Soft Computing Applications (SOFA), Nov. 2020, hybrid.

https://doi.org/10.1007/978-3-031-23636-5_50

2018 **Vulnerabilities of the McEliece Variants Based on Polar Codes**, *Vlad-Florin Drăgoi, Valeriu Beiu, Dominic Bucerzan*, International Conference on Security for Information Technology and Communications (SecITC), November 8–9, 2018, Bucharest, Romania.

https://link.springer.com/chapter/10.1007/978-3-030-12942-2_29

2018 **Survey on Cryptanalysis of Code-Based Cryptography : From Theoretical to Physical Attacks**, *Vlad-Florin Dragoi, Tania Richmond, Dominic Bucerzan and Axel Legay*, IEEE International Conference on Computers Communications and Control, Oradea, Romania, May 2018.

`http://dx.doi.org/10.1109/ICCCC.2018.8390461`

2017 **The Simple Roots Problem**, *Dominic Bucerzan, Vlad-Florin Dragoi and Tania Richmond*, Romanian Cryptology Days (RCD), Sept. 18-20, 2017, Bucharest, Romania.

`http://www.acad.ro/sectii2002/proceedings/doc2017-4s/03artSupl.pdf`

2017 **Evolution of the McEliece Public Key Encryption Scheme**, *Dominic Bucerzan, Vlad-Florin Dragoi and Hervé Talé Kalachi*, International Conference on Security for Information Technology and Communications (SecITC), June 8-9, 2017, Bucharest, Romania.

`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-Florin Dragoi, Ayoub Otmani, Jean-Pierre Tillich*, IEEE International Symposium on Information Theory (ISIT), July 10-15, 2016, Barcelona, Spain.

`http://dx.doi.org/10.1109/ISIT.2016.7541295`

2016 **Weak Keys for the Quasi-Cyclic MDPC Public Key Encryption Scheme**, *Magali Bardet, Vlad-Florin Dragoi, Jean-Gabriel Luque, Ayoub Otmani*, Progress in Cryptology – AFRICACRYPT, April 13-15, 2016, Fes, Morocco.

`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 Chaulet, Vlad-Florin Dragoi, Ayoub Otmani, Jean-Pierre Tillich*, International Workshop on Post Quantum Cryptography (PQCrypt), Feb. 24-26, 2016, Fukuoka, Japan.

`http://dx.doi.org/10.1007/978-3-319-29360-8_9`

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

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

International Conferences : Reliability Theory

2022 **Green AI from Kirchhoff to Shannon**, *Vlad-Florin Dragoi, Mihai Tache, Sorin Hoara, Valeriu Beiu*, , 9th International Conference on Computers Communications and Control (ICCCC) 16-20 May 2022, Oradea, Romania.

`https://link.springer.com/chapter/10.1007/978-3-031-16684-6_37`

2022 **On the Roots of Certain Reliability Polynomials**, *Vlad-Florin Dragoi, Leonard Daus, Marilena Jianu, Dominic Bucerzan, Valeriu Beiu*, 9th International Conference on Computers Communications and Control (ICCCC) 16-20 May 2022, Oradea, Romania.

`https://link.springer.com/chapter/10.1007/978-3-031-16684-6_34`

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.

`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.

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.

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.

https://doi.org/10.1007/978-3-030-53651-0_3

2020 **Consecutive Systems Asymptotic Threshold Behaviors**, *Vlad-Florin Drăgoi, Valeriu Beiu*, International Workshop Soft Computing Applications, Nov. 2020, hybrid.

https://doi.org/10.1007/978-3-031-23636-5_53

2018 **On Posets for Reliability : How Fine Can They Be ?**, *Valeriu Beiu, Simon R. Cowell, Vlad-Florin Dragoi*, International Workshop on Soft Computing Applications SOFA, Sept. 2018, Arad, Romania.

https://doi.org/10.1007/978-3-030-51992-6_10

2018 **Effective Conductances of Moore-Shannon Hammocks**, *Simon R. Cowell, Vlad-Florin Dragoi, Valeriu Beiu, Noemi Rohatinovici*, IEEE International Conference on Nanotechnology (IEEE-NANO), Cork, Ireland, JUL 23-26, 2018.

http://dx.doi.org/10.1109/NANO.2018.8626295

2018 **Ordering Series and Parallel Compositions**, *Vlad-Florin Dragoi, Simon R. Cowell, Valeriu Beiu*, IEEE International Conference on Nanotechnology (IEEE-NANO), Cork, Ireland, JUL 23-26, 2018.

http://dx.doi.org/10.1109/NANO.2018.8626408

2018 **Hammocks versus Hammock**, *Valeriu Beiu, Simon R. Cowell, Vlad-Florin Dragoi, Sorin Hoară and Păstorel Gaşpar*, IEEE International Conference on Computers Communications and Control, Oradea, Romania, May 2018.

http://dx.doi.org/10.1109/ICCCC.2018.8390447

2018 **Can Series and Parallel Compositions Improve on Hammocks ?**, *Vlad-Florin Dragoi, Simon R. Cowell, Valeriu Beiu, Sorin Hoară and Păstorel Gaşpar*, IEEE International Conference on Computers Communications and Control, Oradea, Romania, May 2018.

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-Florin Dragoi and Valentina Emilia Balas*, IEEE International Conference on Computers Communications and Control, Oradea, Romania, May 2018.

http://dx.doi.org/10.1109/ICCCC.2018.8390449

International Journals

2025 **Optimizing Key Recovery in Classic McEliece : Advanced Error Correction for Noisy Side-Channel Measurements**, *Nicolas Vallet, Pierre-Louis Cayrel, Brice Colombier, Vlad-Florin Drăgoi, Vincent Grosso*, IACR Communications in Cryptology, vol. 2, no2, 2025.

https://doi.org/10.62056/ahmpgyl7s

2025 **Weight Structure of Low/High-Rate Polar Codes and Weight Contribution-based Partial Order**, *Mohammad Rowshan, Vlad-Florin Drăgoi*, IEEE Transactions on Information Theory, vol. 71, no. 12,2025.

https://doi.org/10.1109/TIT.2025.3616283

2024 **Integer syndrome decoding in the presence of noise**, *Vlad-Florin Drăgoi, Brice Colombier, Pierre-Louis Cayrel, Vincent Grosso*, Cryptography and Communications, vol. 16, 2024.

https://doi.org/10.1007/s12095-024-00712-3

2024 **On the Closed-form Weight Enumeration of Polar Codes : 1.5d-weight Codewords**, *Vlad-Florin Drăgoi,Mohammad Rowshan, Jinhong Yuan*, IEEE Transactions on Communications, early access, 2024.

https://doi.org/10.1109/TCOMM.2024.3394749

2024 **Which Coefficients Matter Most – Consecutive-k-out-of-n :F Systems Revisited –**, *Vlad-Florin Drăgoi, and Valeriu Beiu*, IEEE Transactions on Reliability, vol. 73, no 3, 2024.

https://doi.org/10.1109/TR.2024.3353908

2023 **The Roots of the Reliability Polynomials of Circular Consecutive-k-out-of-n :F Systems**, *Jianu, Marilena, Leonard Dăuș, Vlad-Florin Drăgoi, and Valeriu Beiu*, Mathematics, vol. 11, no. 20, 2023.

https://doi.org/10.3390/math11204252

2023 **Reliability polynomials of consecutive-k-out-of-n :F systems have unbounded roots**, *Jianu, Marilena, Leonard Dăuș, Vlad-Florin Drăgoi, and Valeriu Beiu*, Networks, vol. 82, 2023.

https://doi.org/10.1002/net.22168

2022 **Fast Reliability Ranking of Matchstick Minimal Networks**, *Vlad-Florin Dragoi, Valeriu Beiu*, Networks, vol. 79, no. 4, 2022.

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

2022 **Profiled Side-channel Attack on Cryptosystems based on the Binary Syndrome Decoding Problem**, *Brice Colombier, Vlad-Florin Dragoi, Pierre-Louis Cayrel, Vincent Grosso*, IEEE Transactions on Information Forensics and Security, vol. 17, 2022.

https://doi.org/10.1109/TIFS.2022.3198277

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.

https://doi.org/10.3390/math9243182

2021 **Reliability of Small Sorting Networks Four Input Sorter Good, Larger Ones Slightly Less So**, *Vlad-Florin Dragoi, Simon Robin Cowell, Valeriu Beiu*, IEEE Transactions on Nanotechnology, vol. 20, 2021.

http://dx.doi.org/10.1109/TNANO.2021.3113731

2021 **Bhattacharyya Parameter of Monomial Codes for the Binary Erasure Channel : From Pointwise to Average Reliability**, *Vlad-Florin Dragoi, Gabriela Cristescu*, Sensors, vol. 21, no. 9, 2021.

`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.

`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.

`https://doi.org/10.15837/ijccc.2020.5.3920`

2020 **Studying the Binary Erasure Polarization Subchannels Using Network Reliability**, *Vlad-Florin Drăgoi, Valeriu Beiu*, IEEE Communications Letters, vol.24, no.1, pp. 62-66, jan. 2020.

`http://doi.org/10.1109/LCOMM.2019.2947910`

2019 **Cubic Spline Approximation of the Reliability Polynomials of Two Dual Hammock Networks**, *Gabriela Cristescu, Vlad-Florin Drăgoi*, TJMM, vol.11, no.1-2, pp. 77-90, 2019.

`http://doi.org/10.1109/LCOMM.2019.2947910`

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

`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-Florin Dragoi, Hervé Talé Kalachi* , IEEE Communications Letters, vol. 22 ,pp. 264-267, Feb. 2018.

`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-Florin Dragoi, Tania Richmond*, International Journal of Computers Communications & Control , vol. 12, no. 1, pp. 7-25, 2017 .

`http://dx.doi.org/10.15837/ijccc.2017.1.2780`