

Vlad-Florin Drăgoi

Education

2013-2016 PhD in Computer Science (Code-Based Cryptography)

Title *Algebraic approach for the study of algorithmic problems coming from cryptography and the theory of error correcting codes*

Advisors Professor Ayoub Otmani and Associate Professor Magali Bardet

Members Prof. Daniel Augot (INRIA Saclay), Prof. Philippe Gaborit (Université de Limoges), Prof. Nicolas Sendrier (INRIA Paris), Prof. Thierry Berger (Université Limoges)

University University of Rouen-Normandy, Saint-Etienne du Rouvray, France

Link <https://hal.archives-ouvertes.fr/tel-01627324/>

2011-2013 MSc in Cryptography and IT Security

Title *Side-channel attacks in code-based cryptography*

Advisors Professor Fabien Laguillaumie and Associate Professor Pierre-Louis Cayrel

University Institut de Science Financière et d'Assurances of the Claude Bernard University Lyon 1, Lyon, France

Link <https://docs.google.com/file/d/0B4Cy03-L745ZZ2pXT1pBTWE2MGM/edit>

2011 BSc in Mathematics

University Claude Bernard University Lyon 1, Villeurbanne, France

Academic Positions

2024- **Vice Dean** Faculty of Exact Sciences at Aurel Vlaicu University of Arad, Romania

2022- **Associate Professor** in Computer Science at Aurel Vlaicu University of Arad, Romania

2018-2021 **Assistant Professor** in Computer Science at Aurel Vlaicu University of Arad, Romania

2018-2020 **Post-Doc Candidate** in a EU project BioCell-NanoART at Aurel Vlaicu University of Arad, Romania

2016-2017 **Assistant Professor (ATER)** in Computer Science at University of Rouen Normandy, France

2013-2016 **PhD candidate** at the University of Rouen Normandy, France

Teaching Activities

2013-2017 **Teaching Assitant** Computer Science Department, University of Rouen Normandy, France.

Introduction to C language (labs) : 18-20 first year students in CS

Web applications (labs) : 18-20 first year students in CS

Computer Graphics (seminars) : 15-18 third year students in CS

2019- **Lecturer** Computer Science Department, Aurel Vlaicu University of Arad, Romania.

Object Oriented Programming (lectures) : 80 second year students in CS

Operating Systems (lectures) : 100 first year students in CS

Information Security and Cryptography (lectures and seminars) : 50 second year students in CS

Automata and Complexity (lectures and seminars) : 50 second year students in CS

Modeling and Simulation Techniques (lectures and seminars) : 50 Master students in CS

Research Activities

Research Projects

2021-2024 Member research project (Romania) : PN-III-P4-ID-PCE-2020-2495.

2020-2022 Director research project (Romania) : PN-III-P1-1.1-PD-2019-0285.

2018 Director research project (Romania) : PN-III-P1-1.1-MC-2018-2769.

2018-2020 Member European research project : POC-A1-A1.1.4-E nr. 30/2016.

Visiting profesor/researcher

2024 10 June-10 July, *Hubert Curien Lab*, Univ. Jean-Monnet, Saint-Etienne, France.

2023 18-28 November, *Wireless Communications Lab*, Univ. of New South Wales, Sydney, Australia.

2023 4-30 September, *LITIS Lab*, Univ. of Rouen Normandy, France.

2023 17 June-17 July, *Hubert Curien Lab*, Univ. Jean-Monnet, Saint-Etienne, France.

Reviews for International Journals

2017- IEEE Communications Surveys and Tutorials, IEEE Transactions on Very Large Scale Integration, IEEE Transactions on Information Theory, IEEE Transactions on Communications, Networks

Presentations/Contributed Talks at Seminars and Summer Schools

2023 Generalized inverses over finite fields : an application to syndrome decoding, *LITIS, Univ. of Rouen Normandy*, Rouen, France.

2023 Secure and reliable post-quantum communications, *Hubert Curie Lab, Univ. Jean-Monnet*, Saint-Etienne, France.

2022 Code-based encryption schemes, *Workshop on Selected Topics in Cryptography*, IMAR, Romania.

2019 Code-based solutions for post-quantum cryptography, *University of Bucharest*, Bucharest, Romania.

2018 Algebraic approach for post-quantum cryptography, *West University of Timișoara*, Rimisoara, Romania.

2015 Clés faibles dans le cryptosystème de QC-MDPC, *Journée des doctorants - LITIS*, Rouen, France.

2015 Cryptographie basée sur les codes correcteurs d'erreurs, *Écoles Jeunes chercheurs Informatique-Mathématique*, Orléans, France.

2015 Polar codes : algebraic structure and properties, *INRIA*, Paris, France.

2014 Lyndon words and weak keys for the QC-MDPC cryptosystem, *INRIA*, Paris, France.

2014 Le problème des polynômes à racines simples sur un corps fini, *Séminaire Imath*, Toulon, France, ([imath website](#)).

2014 Polynomial structures in code-based cryptography, *NORMASTIC- Axe Algorithmique et Combinatoire*, Caen, France, ([normastic website](#)).

Regular Contributions to Seminars

- 2019-** **Scientific seminar**, Computer Science Dept., Faculty of Exact Sciences, Aurel Vlaicu University, Arad, Romania.
- 2014-2017** **Les Séminaires d'Informatique Théorique**, Computer Science Dept., LITIS Lab, University of Rouen-Normandie, France. ([website](#)).

Presentations at International Conferences

- 2013-2024** WSTC 2022, IMACCC 2021, Eurocrypt 2021, ICCCC 2020, SOFA 2018, ICCCC 2018, SecITC 2018 and 2017, ISIT 2016, AFRICACRYPT 2016, PQCrypt 2016, and Indocrypt 2013.

Awards/Scholarships

- 2018** *IEEE Best paper award* for two articles : **Could Series and Parallel Compositions Improve on Hammocks?** and **Survey on Cryptanalysis of Code-Based Cryptography : From Theoretical to Physical Attacks**
- 2018-2023** Rewarding research activity, Ministry of Research, PRECISI : 2018 (1Q2), 2020 (1Q2), 2021 (3 Q1), 2023 (2 Q1, 1Q2)
- 2013-2016** Full PhD scholarship in the former Doctoral School SPMII (Sciences Physiques, Mathématiques et de l'Information pour l'Ingénieur). That year there were only 8 such scholarships for all the students in all the possible research subjects at the University of Rouen, Normandy.

Languages

— Romanian **Native speaker**
— English **Fluent**

— French **Fluent**
— Spanish **Beginner**

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

- 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 Application to 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 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 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 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 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 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 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 Chaleet, Vlad 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 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 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 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 Dragoi, Sorin Hoară and Păstorel Gașpar*, 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 Dragoi, Simon R. Cowell, Valeriu Beiu, Sorin Hoară and Păstorel Gașpar*, 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 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

- 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 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 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 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 Dragoi, Simon R. Cowell, Valeriu Beiu, Sorin Hoară and Păstorel Gaşpar*, 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 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 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>