Aurel Vlaicu University of Arad,
Faculty of Exact Sciences,
Strada Elena Dragoi Nr 2,
Arad, România
vlad.dragoi@uav.ro
Scopus, ORCID, dblp
Google Scholar, Research Gate

Vlad-Florin Drăgoi

Research Interest

Code-based Post-quantum Cryptography Researcher

Researcher in coding theory, cryptography and reliability theory, with expertise in code-based cryptography, side-channel attacks, and polar coding. Active in interdisciplinary research bridging theoretical computer science, information security, and reliable computing systems. International experience in France, Romania, and Australia.

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-L745ZZ2pXTlpBTWE2MGM/edit`

2011 **BSc in Mathematics**

University Claude Bernard University Lyon 1, Villeurbanne, France

Academic Positions

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

2024- **Member of the Research Council** 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

2019-2025 **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
Data Science (lectures and seminars) : 50 Master students in CS

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

2018-2025 **Mentoring**

BSc & Master	25 students - Faculty of Exact Sciences, Aurel Vlaicu Univ. of Arad
Nicolas Vallet (PhD)	Univ. Jean Monnet, Sainte-Etienne France (2023-2025) : *Side-channel attacks against Classic McEliece KEM*
Andreea Szocs	Aurel Vlaicu University, Arad (2021-2023) : *Decreasing Monomial Codes*
Alexandru Popoviciu	Aurel Vlaicu University, Arad (2019-2020) : *Combinatorial Integer syndrome decoding*
Alin Lacatus	Aurel Vlaicu University, Arad (2019-2020) : *Combinatorial Integer syndrome decoding*
Sylvestre Vimard	Univ. Rouen Normadie, France, (2016-2017) : *Étude des structures mathématiques à la base du jeu de Sudoku*
Ph.D.	Andreea Szocs - Univ. of Szeged Doctoral School

Research Activities

Research Projects

2026-2031 Member research project (Romania) : RExQTCS : Centrul Românesc de Excelență în Tehnologii Cuantice cu impact în Securitatea Cibernetică (PN-IV-P6-6.1-CoEx-2024-0214.

2025-2027 Director research project (Romania) : UAV-IRG-1-2025-12.

2025-2025 Director research project (Romania) : PN-IV-P2-2.2-MCD-2025-0506.

2025-2026 Member research project (Romania) : PN-IV-P10-SS-SC-2024-0128.

2024-2025 Member research project France–Czech Rep.–Romania : Barrande+.

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.

2016-2017 Member Projet régional de recherche en Normandie, MOUSTIC-Modèles aléatoires et Outils Statistiques, Informatiques et Combinatoires.

Visiting professor/researcher

2026 **11 May-10 June**, *Hubert Curien Lab*, Univ. Jean-Monnet, Saint-Etienne, France.

2025 **12 May-13 June**, *Hubert Curien Lab*, Univ. Jean-Monnet, Saint-Etienne, France.

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, IEEE Transactions on Reliability, Symmetry, Cryptography

Ph.D. committee

2025 **Alexandru Ionita**, *"Attribute-based Encryption for Boolean Circuits"*, Institutul de Matematica al Acadmiei Romane "Simion Stoilow", Bucharest, Romania, July 2025.

2024 **Oussama Kabbouch**, *"On the decoding by error-correcting pairs and the Galois dual of QT codes"*, Moulay Ismail University, Meknes, Morocco, July 2024.

Presentations/Contributed Talks at Seminaries and Summer Schools

2026 **Code-based cryptosystems in the NIST post-quantum standardization process**, *REx-QTCS : Centrul Românesc de Excelență în Tehnologii Cuantice cu impact în Securitatea Cibernetică - opening conference - Politechnic Univ. of Bucharest*, Bucharest, Romania.

2025 **Fourth round of the NIST post-quantum standardization process**, *Politechnic Univ. of Bucharest*, Bucharest, Romania.

2024 ***Classic McEliece* KEM – the NIST post-quantum standardization process**, *Politechnic Univ. of Bucharest*, Bucharest, Romania.

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**, *Wireless Communication Lab, Univ. New South Wales*, Sydney, Australia.

2023 **Secure and reliable post-quantum communications**, *Hubert Curine 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.

2014 **Polynomial structures in code-based cryptography**, *NORMASTIC- Axe Algorithmique et Combinatoire*, Caen,France.

Regular Contributions to Seminaries

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.

Presentations at International Conferences

2013-2026 SAC 2025, 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.

Organising conferences/special sessions

WSTC 2022 Conference organised together with F. Tiplea

`https://www.wstc.flt-info.eu/spring2022/`

SOFA 2020 Organised two special sessions : Cryptography and Reliability

`https://www.sofa-org.eu/2020/program-and-special-sessions/`

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 fields at the University of Rouen, Normandy.

Languages

— Romanian **Native speaker**

— English **Fluent**

— French **Fluent**

— Spanish **Beginner**