

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

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

Research Activities

Advisor/Co-advisor Ph.D.

2022-2026 Student : Andreea Szöcs

Advisors György Turán and Vlad-Florin Dragoi

University Doctoral School of Computer Science, University of Szeged, Hungary

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

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

2023 **4-30 September**, *C&A research team, LITIS Lab*, Univ. of Rouen Normandy, France.

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

Reviews for International Journals

2017-2022 IEEE Communications Surveys and Tutorials, IEEE Transactions on Very Large Scale Integration, IEEE Transactions on Information Theory, 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 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, ([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

2013-2020 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**