Faculty of Exact Sciences,
Aurel Vlaicu University,

2 Elena Dragoi Street
Arad, Romania
vlad.dragoi@uav.ro
Scopus, ORCID, dblp
Google Scholar, ResearchGate

Vlad-Florin Drăgoi

Education

2013-2016 PhD in Computer Science

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

Positions Held

2018- Senior Lecturer

Teaching Activity Web applications, Operating systems, Object Oriented Programming (freshman and second year students in the Computer Science Departement)

Universitatea Aurel Vlaicu University of Arad, România

2018-2020 Post-Doc Candidate

Research Member of the project "BioCell-NanoART = Novel Bio-inspired Cellular Nano-architectures, POC-A1-A1.1.4-E nr. 30/2016". In this project I investigate the reliability of two-terminal networks, in particular matchstick minimal networks. I explore different techniques for improving and evaluating reliability of networks under constraints, such as probability of failure of devices, number of devices used in the constructions, number of wires necessary for building the structures.

University Aurel Vlaicu University of Arad, Romania

2016-2017 Lecturer

Teaching Member of the Computer Science Department - I taught *Algorithms*, *Web Technologies* (classes of 18-20 freshman students in Computer Science) and *Computer Graphics* (classes of 15 students in third year in BSc in Computer Science).

Research Member of the research team *Combinatoire et Algorithmes*, part of the *Laboratoire d'Informatique, du Traitement de l'Information et des Systèmes* (LITIS). I continued to investigate the security of the latest cryptosystems. One of the main results was a full cryptanalysis of the McEliece variant based on QC-MDPC and QC LDPC codes.

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

2013-2016 PhD candidate

Teaching Member of the Computer Science Department I taught *Introduction to C language* (classes of 18-20 freshman students in Computer Science).

Research I had results in code-based cryptography and related fields like, coding theory and security. One of my most significant contributions to this field was to introduce an algebraic formalism to characterize the structure of polar codes. These results lead to several applications such as an efficient construction method of polar codes, improved decoding techniques, etc. I also used this new formalism to prove the insecurity of a public key cryptosystem based on polar codes. Another contribution that I had during my PhD was to show how to apply combinatorial counting methods to code-based cryptography. Using these methods I managed to reveal and to count the number of weak keys in the McEliece scheme based on QC-MDPC codes.

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

Research Activities

Research Projects

2020 Director research project : PN-III-P1-1.1-PD-2019-0285.

2018 Director Mobility project : PN-III-P1-1.1-MC-2018-2769.

2018-2020 Member of the project "BioCell-NanoART = Novel Bio-inspired Cellular Nano-architectures, POC-A1-A1.1.4-E nr. 30/2016".

2014-2017 Member of Normastic - Fédération Normande de Recherche en Sciences et Technologies de l'Information et de la Communication (FR CNRS 3638). I was a member of the team *Combinatoire et Algorithmes*. Several conferences and publication were partially financed by this project. The list of all publications financed through this project can be found here .

2013-2016 Member of the NATO Project - Secure implementation of post-quantum cryptography, SPS Project Number : 984520 http://old2.re-search.info/

It was an international project between France, Slovakia, USA and Israel. I was part of the French team and some of my publications related to side-channel attacks against the McEliece scheme were financed by this project. For more details on this check the final report (here) .

Reviews for International Journals

2018-2020 IEEE Transactions on Very Large Scale Integration, IEEE Transactions on Information Theory

Presentations at Seminaries and Summer Schools

2019 Code-based solutions for post-quantum cryptography, *Universitatea din Bucureşti*.

2018 Algebraic approach for post-quantum cryptography, *Seminarul ştiinţific - Universitatea de Vest, Timişoara*.

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.

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 Seminaries

2019- **Seminarul stiintific**, Computer Science Dept., Faculty of Exact Sciences, Aurel Vlaicu University, Arad, Romania.

I initiated this scientific seminary for students interested in subjects out-of-the-box. Along with my collegue Simon R. Cowell we lead this seminary and bring into attention subjects that are not usually takeled during the Bachelor of Master degree at our University, e.g., post-quantum cryptography, information theory, network theory, machine learning, etc.

2014-2017 **Les Séminaires d'Informatique Théorique**, Computer Science Dept., LITIS Lab., University of Rouen-Normandie, France. (website).

I was an active member in this project by presenting several research results. I also animated the seminary from 2016 to 2017 and had a principal role in the administration part of the project.

Presentations at International Conferences

2013-2020 I presented the accepted papers in ICCCC2020, SOFA 2018, ICCCC 2018, SecITC 2018 and 2017, ISIT 2016, AFRICACRYPT 2016, PQCrypt 2016, and Indocrypt 2013.

Awards

2018 ICCCC 2018 -*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**

2013-2016 Full PhD scolarship 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.

Communication skills

2015-2016 Member of Science Action - Pôle régional des savoirs - Rouen, France. I had two major communication project : vulgarization of scientific results in a national journal "La science du secret", and explaining to the high-school students of Lycée Marc Bloch, Val-de-Reuil what is the meaning and life of a researcher (here).

Computer skills

- Web Technologies : Ruby on Rails, PHP, HTML, CSS
- IT Security : Bash, Wireshark, PKI, Assembly
- Symbolic computation and statistics : Magma, Maple, PARI/GP, SAS, R
- Object oriented programming : Java
- Data Science : ACP, AFC, AFCM

Languages

- Romanian **Native speaker**
- English **Fluent**
- French **Fluent**
- Spanish **Beginne**