

# Drăgoi Vlad-Florin

## Educație

### 2013-2016 Doctorat în Informatică

Titlu *Approche algébrique pour l'étude et la résolution de problèmes algorithmiques issus de la cryptographie et la théorie des codes*

Îndrumatori Prof. Ayoub Otmani și Conf. Magali Bardet

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

Universitate Universitatea din Rouen-Normandia, Saint-Etienne du Rouvray, Franța

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

### 2011-2013 Master în Matematică Aplicată : Finanțe - Ingineria Riscului, Specializare Securitatea Sistemelor de Informații

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

Îndrumatori Prof. Fabien Laguillaumie și Conf. Pierre-Louis Cayrel

Universitate Institutul de Științe Financiare și de Asigurări al Universității Claude Bernard Lyon 1, Lyon, Franța

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

### 2011 Licență în Matematică

Universitatea Claude Bernard Lyon 1, Villeurbanne, Franța

## Funcții deținute

### 2018-2022 Lector universitar

Activitate didactică *Tehnologii Web, Sisteme de operare, Securitate Informatică, Programare orientată pe obiecte* (Cursuri și laboratoare la anul 1 și 2 de Licență Informatică)

Universitatea Universitatea "Aurel Vlaicu" din Arad, România

### 2020-2022 Director Proiect cercetare

Cercetare Proiectul PN-III-P1-1.1-PD-2019-0285 intitulat "Metode algebrice pentru evaluarea securității criptosistemelor post-cuantice bazate pe teoria codurilor corectoare de erori" are ca scop studierea securitatii criptosistemelor post-cuantice bazate pe coduri corectoare de erori.

Universitatea Universitatea "Aurel Vlaicu" din Arad, România

### 2018-2020 Cercetător Post-Doc

Cercetare Membru în proiectul "BioCell-NanoART = Novel Bio-inspired Cellular Nano-architectures, POC-A1-A1.1.4-E nr. 30/2016". În cadrul acestui proiect studiez fiabilitatea unor rețele, denumite "Matchstick Minimal Networks".

Universitatea Universitatea "Aurel Vlaicu" din Arad, România

## 2016-2017 Asistent universitar

Activitate didactică *Algoritmi și Tehnologii Web* (Laboratoare și seminarii la grupe de 18-20 studenți din anul 1 de Licență), *Infografie* (Seminarii la grupe de 15 studenți din anul 3 de Licență în Informatică).

Cercetare Am făcut parte din echipa de cercetare *Combinatoire et Algorithmes*, a laboratorului de cercetare *Laboratoire d'Informatique du Traitement de l'Information et des Systèmes* (LITIS). Cercetarea mea s-a concentrat în mare parte pe analiza securității ultimelor criptosisteme de tip McEliece.

Universitate Universitatea din Rouen-Normandia, Saint-Etienne du Rouvray, Franța

## 2014-2016 Asistent universitar

Activitate didactică *Introducere în limbajul C și Tehnologii Web* (Seminarii și laboratoare la grupe de 18-20 studenți din anul 1 de Licență).

Cercetare În laboratorul LITIS, subiect de cercetare : criptografie post-cuantică.

Universitate Universitatea din Rouen-Normandia, Saint-Etienne du Rouvray, Franța

## 2013-2016 Doctorant

Cercetare În laboratorul LITIS, subiect de cercetare : criptografie post-cuantică.

Universitate Universitatea din Rouen-Normandia, Saint-Etienne du Rouvray, Franța

---

## Activități de cercetare

### Proiecte de cercetare

2021-2024 Membru proiect de cercetare : PN-III-P4-ID-PCE-2020-2495.

2020-2022 Director proiect de cercetare : PN-III-P1-1.1-PD-2019-0285.

2018 Director proiect de mobilitate : PN-III-P1-1.1-MC-2018-2769.

2018-2020 Membru in proiect de cercetare : POC-A1-A1.1.4-E-2015 nr. 30/01.09.2016.

2016-2019 Membru într-un proiect de cercetare în Normandia, Franța, intitulat **MOUSTIC**-Modèles aléatoires et Outils Statistiques, Informatiques et Combinatoires. <http://gpm.univ-rouen.fr/en/node/93>

2013-2016 Membru al unui proiect NATO "Secure implementation of post-quantum cryptography", SPS Project Number : 984520.

### Recenzii pentru jurnale internaționale

2018-2022 IEEE Communications Surveys and Tutorials, IEEE Transactions on Very Large Scale Integration, IEEE Transactions on Information Theory, MDPI Cryptography, MDPI Symmetry

### Invitat cu prezentări la seminarii și școli de vara

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

2018 **Algebraic approach for post-quantum cryptography**, *Seminarul științific - Universitatea de Vest, Timișoara*.

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

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

2014 **Le problème des polynômes à racines simples sur un corps fini**, *Séminaire Imath, Toulon, Franța*.

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

### Comitet organizare evenimente științifice

- 2022 Workshop on Selected Topics in Cryptography - Sesiunea primavara 2022
- 2020 SOFA 2020, Special session - Advances in Cryptology : from theory to practice
- 2020 SOFA 2020, Special session - Rebooting Reliability – From Maths to Circuits

### Contribuții regulate la seminarii

- 2019-2022 **Seminarul științific**, Facultatea de științe Exacte, Universitatea Aurel Vlaicu, Arad, Romania.  
Am initiat seminarul stiintific pentru studentii interesati de subiecte diferite de ce se preda in mod obisnuit. Impreuna cu colegul meu Simon R. Cowell propunem studentilor prezentari pe subiecte cum ar fi, criptografia post-cuantica, teoria informatiei, network theory, etc.
- 2014-2017 **Les Séminaires d'Informatique Théorique**, Laboratorul LITIS, Universitatea din Rouen-Normandia, Franța.  
Am fost membru activ al acestui seminar unde am prezentat de nenumărate ori rezultatele mele de cercetare. Am fost unul dintre organizatorii principali ai acestui seminar din 2016 până în 2017.  
<https://dpt-info-sciences.univ-rouen.fr/index.php/la-recherche/seminaires>

### Prezentări la conferințe internaționale

- 2013-2018 Am prezentat articolele acceptate la IMACCC2021, SOFA 2018, ICCCC 2018, SecITC 2017, SecITC 2018, ISIT 2016, AFRICACRYPT 2016, PQCrypt 2016, Indocrypt 2013.

---

### Premii și burse

- 2018 IEEE Best paper award pentru două lucrări : **Could Series and Parallel Compositions Improve on Hammocks?** și **Survey on Cryptanalysis of Code-Based Cryptography : From Theoretical to Physical Attacks**
- 2018-2022 Premiera rezultatelor cercetării UEFISCDI - Articole, Competiția 2018 (1 Galben), 2020 (1 Galben), 2021 (3 Rosii)
- 2013-2016 Bursă de doctorat pentru finanțarea celor 3 ani de teză câștigată în urma unui concurs. În anul 2013 școala doctorală SPMII (Sciences Physiques, Mathématiques et de l'Information pour l'Ingénieur), actuala MIIS (Mathématiques, Information, Ingénierie des Systèmes) a acordat per total doar 8 astfel de burse pentru toate domeniile de cercetare.

---

### Comunicare

- 2015-2016 Membru al [Science Action](http://www.scienceaction.asso.fr/) (<http://www.scienceaction.asso.fr/>)  
Pôle régional des savoirs - Rouen, Franța. Am avut două proiecte de comunicare : primul a constat în vulgarizarea rezultatelor științifice și publicarea acestora într-un jurnal francez "[La science du secret](http://www.scienceaction.asso.fr/ressources/formation-des-doctorants/vlad-d-la-science-du-secret)" (<http://www.scienceaction.asso.fr/ressources/formation-des-doctorants/vlad-d-la-science-du-secret>) iar al doilea au fost o serie de prezentări în fața unor clase de liceu a vieții de cercetător, de exemplu la liceul Marc Bloch, Val-de-Reuil ([aici](http://www.scienceaction.asso.fr/evenements/forums-jeunes/val-de-reuil-lyc%C3%A9e-marc-bloch-5)) <http://www.scienceaction.asso.fr/evenements/forums-jeunes/val-de-reuil-lyc%C3%A9e-marc-bloch-5>.

## Competențe Informatică

- Tehnologii Web : **Ruby on Rails, PHP, HTML, CSS**
- Securitate IT : **Bash, Wireshark, PKI, Assembly**
- Software (calcul simbolic, numeric, statistică) : **Magma, Maple, PARI/GP, SAS, R**
- Programare orientată pe obiect : **Java**
- Analiză de date (Data science) : **ACP, AFC, AFCM**

## Limbi

- Română **Maternă**
- Engleză **Avansat**
- Franceză **Avansat**
- Spaniolă **Începător**

## Hobiuri

- Volei
- Judo
- Gastronomie
- Musică