Curriculum Vitae

First name: FERUCIO
Middle name: LAURENTIU
Last name: ŢIPLEA

Current Position:
Professor
Department of Computer Science
Alexandru Ioan Cuza University of Iasi
Iasi 700506, Romania
Tel: +40-(0)742-019593
E-mail: ferucio.tiplea@uaic.ro
fltiplea@gmail.com
URL: https://profs.info.uaic.ro/~fltiplea/

Home address:
Str. A. Panu 40
Bl. A. Panu 1A, Ap. 13
Iasi 700020, Romania
Phone: +(40)-0)742-019593

Citizenship: Romanian

Place and date of birth:
Place of birth: Birlad, District of Vaslui, Romania
Date of birth: October 4, 1962
Male/Female: Male

Marital status: Married, one son

Education:

- April 1993: Ph.D., Computer Science
  - Alexandru Ioan Cuza University of Iasi, Romania
  - Ph.D. Thesis on extensions of Petri nets
- June 1986: M.S., Computer Science
  - Alexandru Ioan Cuza University of Iasi, Romania
  - M.S. Thesis on unification algorithms in equational theories

Research Interests:

- Theories and tools for high-level modeling, design, and analysis of systems (including Petri nets and formal verification)
- Cryptography and computer security

Academic Positions:

1. June 2018 – present: Ph.D. supervisor, Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania;
2. Nov 2000 – June 2018: Ph.D. supervisor, Department of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania;
3. Nov 1999 – present: Professor, Department of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania;
4. Oct 1995 – Nov 1999: Associate Professor, Department of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania;
5. Feb 1992 – Oct 1995: Lecturer, Department of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania;
6. July 1991 – Feb 1992: Assistant Professor, Department of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania;
7. Oct 1990 – July 1991: Assistant Professor, Department of Mathematics, Alexandru Ioan Cuza University of Iasi, Romania.

Other Positions:

1. April 1990- Oct 1990: Researcher, Computer Science Research Centre, Alexandru Ioan Cuza University of Iasi, Romania;
2. Sept 1989- April 1990: Mathematician, Research Institute for Electronics, Iasi, Romania;
3. Sept 1986- Sept 1989: Computer Programmer, Computer Science Centre, District of Vaslui, Romania.

Visiting Appointments:

Visiting Professor

- LACL, University Paris 12 Val de Marne, Creteil, France
- September 2008

Visiting Professor

- School of Computer Science, University of Central Florida, Florida, USA
- December 21, 2003 – May 6, 2006

Visiting Scientist

- Department of Computer Science, Carnegie Mellon University, Pittsburg, Pennsylvania, USA
- October 1 - November 30, 2001

Fulbright Fellow

- Department of Computer Science, Carnegie Mellon University, Pittsburg, Pennsylvania, USA
- January 15 - April 14, 2001

German Academy Fellow

- Institut fur Informatik, Universitat Augsburg, Germany
- September 20, 1999 - March 20, 2000

DAAD Fellow

- Institut fur Informatik, Universitat Eichstadt, Germany
- June 30 - August 30, 1999

Monbusho Fellow

- Department of Computer Science, Kyoto Sangyo University, Japan
- October 1995 - March 1997

DAAD Fellow

- Institute fur Informatik, Universitat Freiburg, Germany
- May 1 – July 31, 1995

Teaching:

Network Security (graduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Spring 2010 –)

Algebraic Foundations of Computer Science (undergraduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Fall 1994 – 2003; Spring 2000 –)

Information Security (undergraduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Spring 2008 –)

Decidability and Complexity (undergraduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Fall 1992 – 1998, 2000 – 2003, 2006 –)

Coding Theory and Cryptography / Introduction to Cryptography (undergraduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Spring 1994 – 2002; Fall 2003, 2006 –)

Security Protocols (graduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Spring 2000, 2001; Fall 2002; Spring 2005 – 2007)

Verification techniques for Security Protocols (graduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Fall 2006 – 2008)

Introduction to Discrete Structures (COT3100H) (honors course)

- School of Computer Science, University of Central Florida (The Burnett Honors College)
    - (Spring 2006)

Formal Languages and Automata COT5310 (graduate course)

- School of Computer Science, University of Central Florida
    - (Spring 2005; Fall 2005)

Program Analysis COP5021 (graduate course)

- School of Computer Science, University of Central Florida
    - (Fall 2004; Spring 2006)

Program Analysis (Ph.D. course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Fall 2005; Spring 2008, 2009)
- LACL, University Paris 12 Val de Marne, France
    - (September 2008)

Numerical Calculus COT4500 (undergraduate course)

- School of Computer Science, University of Central Florida
    - (Spring 2004)

Electronic Commerce (graduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Spring 2001)

Data Compression (undergraduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Spring 2001)

Petri Nets (graduate seminar)

- Institut für Informatik, Universität Augsburg, Germany
    - (Fall 1999)

Distributed Systems: Modeling and Analysis with Petri Nets (graduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Spring 1997, 1998, 1999)

Fractal Theory (undergraduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Spring 1996)

Introduction to Computer Science (undergraduate course)

- Faculty of Sociology, Alexandru Ioan Cuza University of Iasi, Romania
- (Fall 1992, 1993, 1994)

Logic Programming (undergraduate course)

- Faculty of Computer Science, Alexandru Ioan Cuza University of Iasi, Romania
    - (Spring 1991, 1992, 1993, 1994)

PhD Students[1]:

1. **Current PhD Students:**

- Cristian Hristea (since Fall 2016)
    - Main topic: cryptography
- George Teseleanu (since Fall 2015)
    - Main topic: cryptography

2. **Former PhD Students:**

- Catalin Lita
    a. PhD Thesis: Malware Detection and Analysis
    b. Institute: Alexandru Ioan Cuza of Iasi, Romania
    c. Date: Oct 2018
- Iulian Goriac
    a. PhD Thesis: An Epistemic Logic Based Framework for Reasoning about Information Hiding
    b. Institute: Alexandru Ioan Cuza University of Iasi
    c. Date: March 2015

[1] The regulations in Romania allowed a faculty to conduct a Ph.D. thesis only few years after being promoted to the rank of Full Professor. I was allowed to supervise Ph.D. students in late 2000 (OMEN no. 4211/20.07.2000).

- Catalin Dragan
    a. PhD Thesis: Security of the CRT-based Secret Sharing Schemes
    b. Institute: Alexandru Ioan Cuza University of Iasi
    c. Date: September 2013
- Cosmin Varlan
    a. PhD Thesis: Anonymity in Security Protocols
    b. Institute: Alexandru Ioan Cuza University of Iasi
    c. Date: April 2013
- Corina Dima (married Bocaneala)
    a. PhD Thesis: Workflow Nets with time, Resource, and Priority Constraints
    b. Institute: Alexandru Ioan Cuza University of Iasi
    c. Date: Martie 1, 2013
- Mogos Gabriela
    a. PhD Thesis: Quantum Cryptography
    b. Institute: Alexandru Ioan Cuza University of Iasi
    c. Date: January 2010
- Constantin Enea
    a. PhD Thesis: Verification by Abstraction
    b. Institute: Univ. Paris 12 Val de Marne
    c. Date: January 2008
    d. Degree: “Tres Honorable”
- Geanina Macovei
    a. PhD Thesis: Timed Petri Nets and Workflow Nets
    b. Institute: Alexandru Ioan Cuza University of Iasi
    c. Date: January 2008
- Sorin Iftene
    a. PhD Thesis: Secret Sharing Schemes with Application in Security Protocols
    b. Institute: Alexandru Ioan Cuza University of Iasi
    c. Date: January 2007
- Catalin Birjoveanu
    a. PhD Thesis: Secrecy for Security Protocols
    b. Institute: Alexandru Ioan Cuza University of Iasi
    c. Date: January 2007

Honor Students (under my supervision, these students have published research papers in international conferences and journals):

1. Alexandru Ionita (SECRYPT 2020)
2. Diana Bolocan (RCD 2019)
3. Victor Pescaru (MFOI 2019)
4. Victor Talif (SECITC 2018)
5. Daniel Plecan (RCD 2017)
6. Lucian Ostepoc (SECITC 2016)
7. Adrian Schipor (BalkanCryptSec 2014, SECITC 2018)
8. Raluca Chirosca (IEEE SMCA 45(9), 2016)
9. Gabriel Nastase (SECITC 2015)
10. Mihai Barzu (Inf. Sciences 240, 2013)
11. Loredana Vamanu (FGCS 29(3), 2013)
12. Constantin Dragan (SECRYPT 2009)
13. Raluca Diaconu (IEEE SMCA 45(3), 2015)
14. Ioana Boureanu (Journal of Computer Security 16(6), 2008)
15. Elena Erbiceanu (June 2005)
16. Claudia Prajescu, Razvan Zlavog (June 2004)
17. Constantin Enea, Dragos Trinca, Bogdan Pasaniuc, Ionut Popa (June 2003)
18. Bernard Ciurariu, Roxana Melinte, Ioana Olga, Olivia Onea (June 2002)
19. Cristina Badarau (Acta Cybern, 2000), Corina Apachite (September 2001)
20. Sorin Iftene (June 2000)
21. Cristian Ioan (February 1999)
22. Hollo Csaba (June 1996)
23. Magdalena Ionescu, Octavian Procopiuc, Cristian Ene, Codrut Matei, Cristian Preda, Geanina Macovei (June 1995)

Contracts, Projects, and Grant Support:

1. Project member: „*EBSIS-Event-based Systems in Iasi*", 2016-2018, under H2020-TWINN-2015, Euro 867,205

2. Project „Practical Escrow-free Identity-based Mutual Authentication and Key Management without Pairings", acronim IB-MAKE, Program „Parteneriate în domenii prioritare", code PN-II-PT-PCCA-2013-4-1651, contract no. 17/2014
    - Funded by UEFISCDI (Romania): Ron 1,437,491 (~ Euro 320,000)
    - Project director
3. COST Action IC 1306: Cryptography for Secure Digital Interaction (Nov 2013 – 2017)
    - Member of the Management Committee
4. Programme "Hubert Curien (PHC) - Brancusi" (May 2013 – Dec 2014)
    - Funded by UEFISCDI (Romania) and EGIDE (France)
    - Director of the Romanian team
5. Integrated Platform for Advanced Studies in Molecular Nanotechnologies (AMON)
    - Coordinator of administrative activities
    - The Platform started in 2006
    - By 2011, it attracted financial support of over Ron 20,000,000 (this is more than Euro 4,000,000)
6. NATO Advanced Research Workshop on Information Security in Wireless Networks (September 4-8, 2006, Suceava, Romania)
    - Funded by NATO Security Through Science Programme;
    - Member of the organizing committee and invited speaker;
7. NATO Advanced Research Workshop *"Verification of Infinite-state Systems with Applications to Security VISSAS 2005"* (March 17-22, Timisoara, Romania)
    - Funded by NATO Security Through Science Programme. Total funding: EUR 35000;
    - NATO co-director;
8. *Modeles executables et verifiables pour la securite des systemes communicants* (2004-2005)
    - Program ECO-NET in cooperation with University Paris 12 (France) and Institute e-Austria Timisoara (Romania);
    - Funded by EGIDE (France). Total funding for 2004: EUR 27400; total funding for 2005: EUR 23684;
    - Co-PI

9. *Modeling and Analysis Techniques for Cryptographic Security Protocols* (2004-2006)
    - by National University Research Council of Romania CNCSIS 632/28/2004 and CNCSIS 632/50/2005;
    - PI;
10. NATO Advanced Research Workshop *"Concurrent Information Processing and Computing 2003"* (July 5-10, Sinaia, Romania)
    - Funded by NATO Security Through Science Programme. Total funding: EUR 30000;
    - NATO co-director;
11. *Security Protocols* (2002-2003)
    - by National University Research Council of Romania – Grant MEC 569, no. 10, 333531/2002;
    - PI;
12. *Topics in Formal Methods of System Design, Analysis, and Verification*
    - by National University Research Council of Romania - every year, since 1990;
    - Co-PI.

Activities at National Level:

1. Member of the Computer Science section of the National Council for the Attestation of University Titles, Diplomas and Certificates (CNATDCU) (2017 – 2018)
2. President of the Computer Science section of the National Council for the Attestation of Academic Degrees, Diplomas and Certificates (CNATDCU) (2016 – 2017)
3. Member of the Computer Science section of the National Council for the Attestation of University Titles, Diplomas and Certificates (CNATDCU) (2011 - 2013)
4. Member of the National University Research Council of Romania (2005 – 2009)
5. Member of the promotion committee for academic positions: C. Popescu (2004), A. Paun (2012, 2014), L. Leustean (2014), A. Popa (2017), C. Muresan (2019), R. Olimid (2019)

Departmental Activities:

1. Director of the Master Program "Information Security" (I initiated the master's program and have been running it since 2010)
2. Member of the promotion committee for academic positions (1997, 2000, 2001, 2002, 2003, 2007, 2009, 2010, 2012, 2013)

3. Committee on M.S. Programs (1998, 2000, 2001, 2006, 2007, 2008, 2012, 2016, 2018, 2019, 2020)
4. Committee on Ph.D. Programs (1998, 2000, 2001, 2002, 2003, 2004, 2006, 2007, 2008, 2011, 2012, 2013, 2015, 2018, 2020)

Professional Activities:

1. Program Committees

- Romanian Cryptology Days (RCD) Conference Series, 2015, 2017, 2019
- International Conference on Security for Information Technology and Communications – SECITC, 2017, 2018, 2019, 2020
- Federated Conference on Computer Science and Information Systems FedCSIS, Cryptography and Security Systems C&SS, 2017, 2018, 2019
- (Co-chair) 3rd International Conference on Cryptography and Information Security BalkanCryptSec, Bucharest, Romania, Sept 8-9, 2018
- 2nd International Conference on Cryptography and Information security BalkanCryptSec, Koper, Slovenia, Sept 3-4, 2015
- 1st International Conference on Cryptography and Information security BalkanCryptSec, Istanbul, Turkey, October 16-17, 2014
- International Workshop on Modeling and Business Environments ModBE'13, Milano, Italy, June 24, 2013
- 5th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2009), Rende, Cosenza, Italy, Sept 21 - 23, 2009
- International Workshop "Formal Methods for Aerospace", satellite workshop of Formal Methods 2009, Eindhoven (the Netherlands), Nov 3, 2009
- International Conference on Security and Cryptography SECRYPT 2009, Milan (Italy)
- International Workshop on Petri Nets and Software Engineering PNSE 2009 (Paris, France, June 22/23, 2009), a satellite event of Petri Nets 2009 30th International Conference on Application and Theory of Petri Nets and Other Models of Concurrency
- International Workshop on Petri Nets and Distributed Systems PNDS 2008 (Xi'an, China, June 23-24, 2008), a satellite event of Petri Nets 2008 29th International

Conference on Application and Theory of Petri Nets and Other Models of Concurrency

- International Conference on Security and Cryptography SECRYPT 2007, Barcelona (Spain)
- Co-chair of the 2nd International Workshop on Petri Nets and Their Applications to Workflow Management, Timisoara (Romania), Sept 2006
- Co-chair of the 1st International Workshop on Information and Computer Security ICS 2006, Timisoara (Romania), Sept 2006
- Member of the organizing committee of the NATO Advanced Research Workshop on Information Security in Wireless Networks (September 4-8, 2006, Suceava, Romania), http://iwiswn.usv.ro/
- Co-chair of the 1st International Workshop on Petri Nets and Their Applications to Workflow Management, Timisoara (Romania), Sept 2005
- NATO co-director and general chair for the Advanced Research Workshop on *Verification of Infinite State Systems with Applications to Security VISSAS 2005*, March 17-22, 2005, Timisoara (Romania)
- 2nd International Workshop on Applications of Petri Nets to Coordination, Workflow and Business Process Management, Miami (Orlando), June 20, 2005
- 6th International Workshop on *Symbolic and Numeric Algorithms for Scientific Computing SYNASC04*, Timisoara (Romania), Sept 26-30, 2004
- International Workshop on *Computer-Aided Verification of Information Systems CAVIS 2004*, Timisoara (Romania), Sept 26-30, 2004
- International Conference on *Computers and Communications ICCC 2004*, Baile Felix Spa-Oradea (Romania), May 27-29, 2004
- 5th International Workshop on *Symbolic and Numeric Algorithms for Scientific Computing SYNASC03*, Timisoara (Romania), Oct 1-4, 2003
- International Workshop on *Computer-Aided Verification of Information Systems CAVIS 2003*, Timisoara (Romania)
- NATO co-director for the Advanced Research Workshop on *Concurrent Information Processing and Computing CIPC2003*, July 5-10, 2003, Sinaia (Romania)
- International Symposium on *Parallel and Distributed Computing*, ECIT, July 2002
- Romanian Symposium on *Computer Science ROSYCS'98*, Iasi (Romania), May 1998
- Romanian Symposium on *Computer Science ROSYCS'96*, Iasi (Romania), May 1996

2. Managing Editor

- Scientific Annals of the Alexandru Ioan Cuza University of Iasi, Computer Science Section (until 2007)

3. Editor
   - Scientific Annals of the Alexandru Ioan Cuza University of Iasi, Computer Science Section
4. Journal Referee
   - Acta Informatica, Fundamenta Informaticae, Information Processing Letters, Information Sciences, Theoretical Computer Science, Acta Cybernetica, IEEE Journal on Computing, IEEE Transactions on Computers, IEEE Transactions on SMCA, International Journal of Foundations of Computer Science, Information Sciences, IEEE Transactions on Services Computing, Transactions on Petri Nets and Other Models of Concurrency (ToPNoC)
5. Professional Organizations
   - American Mathematical Society, European Association for Theoretical Computer Science, Petri Net Special Interest Group, founder member of the National Society for Cryptology
6. Reviewer
   - Zentralblatt fur Mathematik, Mathematical Reviews, Computing Reviews

Invited Talks and Lectures at Universities and Professional Meetings:

1. Invited speaker at the 9th Congress of the Romanian Mathematicians, Galati, Romania, 2019 (talk: Quadratic Residuosity Based Cryptography)
2. Invited speaker at the Romanian Cryptology Days 2019, Sept 18-20, 2019, Bucharest, Romania, http://www.sie.ro/RCD/index.html (talk: Lessons to be Learned for a Good Design of RFID Schemes)
3. Invited speaker at the Conference on Mathematical Foundations of Informatics, July 2 – 6, 2018, Chisinau, Republic of Moldova (talk: Multi-linear Maps in Cryptography)
4. Invited speaker at the Romanian Cryptology Days 2017, Sept 18-20, 2017, Bucharest, Romania, http://www.sie.ro/RCD/index.html (talk: Unpredictability of Jacobi Sequences)
5. Invited talk at the International Conference on Security for Information Technology and Communications – SECITC 2017, June 8-9, Bucharest, Romania (talk: Key-policy Attribute-based Encryption from Bilinear Maps)
6. Invited talk at the Faculty of Computer Science, University of Dresden – April 2017, EBSIS project, (talk: Complexity of anonymity for security protocols)

7. Invited talk at the Faculty of Computer Science, University of Dresden – April 2017, EBSIS project (talk: Sharing Secrets on Boolean Circuits: Application to Key-policy Attribute-based Encryption)
8. Invited talk at the International Conference on Security for Information Technology and Communications – SECITC 2016, June 9-10, Bucharest, Romania (talk: Security of Identity-Based Encryption Schemes from Quadratic Residues)
9. Invited talk at the International Conference on Security for Information Technology and Communications – SECITC 2015, June 11-12, Bucharest, Romania (talk: New Results for Identity-based Encryption from Quadratic Residuosity)
10. Invited speaker at the Romanian Cryptology Days 2015, Sept 21-23, 2015, Bucharest, Romania, http://www.sie.ro/RCD/index.html (talk: Attribute-based Encryption)
11. Invited talk at the Workshop on Circuits, Systems and Information Technology, WCSIT 2014 (talk: The way to modern cryptography)
12. Invited speaker at the Romanian Cryptology Days 2013, Sept 16-17, 2013, Bucharest, Romania, http://www.sie.ro/RCD/index.html (talk: Identity-based Encryption)
13. Invited speaker at the Romanian Cryptology Days 2011, Oct 11-12, 2011, Bucharest, Romania, http://www.sie.ro/RCD/index.html (talk: Modeling and Analysis of Security Protocols)
14. Invited talk at "Laboratoire d'Informatique Algorithmique: Fondements et Applications (LIAFA)" (Université Paris Diderot - Paris 7, France), on *Complexity of anonymity for Security Protocols*, Dec 13, 2010, http://www.liafa.jussieu.fr/
15. Invited Professor at the Doctoral School of LACL, Univ. Paris 12 (September 2008), http://lacl.univ-paris12.fr/
16. Invited talk at the NATO Advanced Research Workshop on Information Security in Wireless Networks (September 4-8, 2006, Suceava, Romania), http://iwiswn.usv.ro/
17. Invited talk at VERIMAG (Grenoble, France) on *Abstractions of Data Types*, July 11, 2005, http://www-verimag.imag.fr/SEMINAIRES/05/
18. Invited talk at the NATO Advanced Research Workshop *Verification of Infinite-state Systems with Applications to Security VISSAS 2005*, Timisoara (Romania), March 17-22, 2005
19. Invited talk at University of Central Florida, School of Computer Science, on *Abstraction Techniques for Program Analysis*, Sept 24, 2004
20. Invited talk at University of Central Florida, School of Computer Science, on *Modeling and Verification of Security Protocols*, June 28, 2004
21. SVC talk at Carnegie-Mellon University on *Abstractions of Data Types*, Pittsburgh (USA), May 4, 2004, http://www-2.cs.cmu.edu/~svc/

22. Invited talk at the NATO Advanced Research Workshop *Concurrent Information Processing and Computing CIPC 2003*, Sinaia (Romania), July 5-10, 2003
23. Invited talk at the *Austrian Workshop on Computer-Aided Verification of Information Systems CAVIS 2003*, Timisoara (Romania), 2003
24. Invited talk at Carnegie-Mellon University, January 2001 and October 2001
25. Invited talk at Jozsef Attila University of Szeged on *Petri Net Reactive Modules*, Szeged (Hungary), 2001
26. Advanced research seminar on *Petri Nets*, Augsburg (Germany), Nov 1999 - Feb 2000
27. Invited talk at Katholische Universitaet Eichstaett-Ingolstadt, Eichstaett (Germany), 1999
28. Invited talk and lectures at Kyoto Sangyo University, Kyoto (Japan), 1996
29. Invited talk at the *Symposium on Semigroups, Languages and Related Fields*, Shimane University (Japan), 1995
30. Invited talk at the *Workshop on Semigroups, Formal Languages and Computer Systems*, Kyoto Sangyo University, Kyoto (Japan), 1995
31. Invited talk at Freiburg University, Freiburg (Germany), 1995

Oct 5, 2021

Prof.dr. Ferucio Laurentiu Tiplea