Curriculum Vitae

First name: FERUCIO
Middle name: LAURENTIU
Last name: TIPLEA

Current Position:

Professor
Department of Computer Science
"Al.I.Cuza" University of Iasi
Iasi 700506, Romania
Tel: +40-232-201538
Fax: +40-232-215199
E-mail: fltiplea@info.uaic.ro
fltiplea@gmail.com
URL: http://www.infoiasi.ro/~fltiplea

Home address:

Str. A. Panu 40
Bl. A. Panu 1A, Ap. 13
Iasi 700020, Romania
Phone: +40-232-211081

Citizenship: Citizen of Romania

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
  - "Al.I.Cuza" University of Iasi, Romania
  - Ph.D. Thesis on extensions of Petri nets
- June 1986: M.S., Computer Science
  - "Al.I.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);
- Variable length codes and applications;
- Cryptography and computer security;

Academic Positions:

1. Nov 2000- present: Ph.D. supervisor, Department of Computer Science, "Al.I.Cuza" University of Iasi, Romania;
2. Nov 1999- present: Professor, Department of Computer Science, "Al.I.Cuza" University of Iasi, Romania;
3. Oct 1995- Nov 1999: Associate Professor, Department of Computer Science, "Al.I.Cuza" University of Iasi, Romania;
4. Feb 1992- Oct 1995: Lecturer, Department of Computer Science, "Al.I.Cuza" University of Iasi, Romania;
5. July 1991- Feb 1992: Assistant Professor, Department of Computer Science, "Al.I.Cuza" University of Iasi, Romania;
6. Oct 1990- July 1991: Assistant Professor, Department of Mathematics, "Al.I.Cuza" University of Iasi, Romania.

Other Positions:

1. April 1990- Oct 1990: Researcher, Computer Science Research Centre, "Al.I.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, “Al.I.Cuza" University of Iasi, Romania
    - (Spring 2010 –)

Algebraic Foundations of Computer Science (undergraduate course)

- Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania
    - (Fall 1994 – 2003; Spring 2000 –)

Information Security (undergraduate course)

- Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania
    - (Spring 2008 –)

Decidability and Complexity (undergraduate course)

- Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania
    - (Fall 1992 – 1998, 2000 – 2003, 2006 –)

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

- Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania
    - (Spring 1994 – 2002; Fall 2003, 2006 –)

Security Protocols (graduate course)

- Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania
    - (Spring 2000, 2001; Fall 2002; Spring 2005 – 2007)

Verification techniques for Security Protocols (graduate course)

- Faculty of Computer Science, "Al.I.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, "Al.I.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, "Al.I.Cuza" University of Iasi, Romania
    - (Spring 2001)

Data Compression (undergraduate course)

- Faculty of Computer Science, "Al.I.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, "Al.I.Cuza" University of Iasi, Romania
    - (Spring 1997, 1998, 1999)

Fractal Theory (undergraduate course)

- Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania
    - (Spring 1996)

Introduction to Computer Science (undergraduate course)

- Faculty of Sociology, "Al.I.Cuza" University of Iasi, Romania
- (Fall 1992, 1993, 1994)

Logic Programming (undergraduate course)

- Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania
    - (Spring 1991, 1992, 1993, 1994)

PhD Students[1]:

[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.

1. **Current PhD Students:**
   - Cristian Hristea (since Fall 2016)
     - Main topic: cryptography
   - Doru Călcâi (since Fall 2016)
     - Main topic: cryptography
   - George Teseleanu (since Fall 2015)
     - Main topic: cryptography
   - Anca Nica (since Fall 2014)
     - Main topic: cryptography
   - Ioana Leahu (since Fall 2013)
     - Main topic: Petri nets
   - Bogdan Prelipcean (since Fall 2013)
     - Main topic: malware
   - Violeta Tulceanu (since Fall 2011)
     - Main topic: brainwave computer interface
   - Catalin Lita (since Fall 2011)
     - Main topic: malware

2. **Former PhD Students:**
   - Iulian Goriac
     a. PhD Thesis: An Epistemic Logic Based Framework for Reasoning about Information Hiding
     b. Institute: "Al.I.Cuza" University of Iasi
     c. Date: March 2015
   - Catalin Dragan
     a. PhD Thesis: Security of the CRT-based Secret Sharing Schemes
     b. Institute: "Al.I.Cuza" University of Iasi
     c. Date: September 2013
   - Cosmin Varlan
     a. PhD Thesis: Anonymity in Security Protocols
     b. Institute: "Al.I.Cuza" University of Iasi
     c. Date: April 2013
   - Corina Dima (Cas. Bocaneala)

    a. PhD Thesis: Workflow Nets with time, Resource, and Priority Constraints
    b. Institute: “Al.I.Cuza” University of Iasi
    c. Date: Martie 1, 2013
- Mogos Gabriela
    a. PhD Thesis: Quantum Cryptography
    b. Institute: “Al.I.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: “Al.I.Cuza” University of Iasi
    c. Date: January 2008
- Sorin Iftene
    a. PhD Thesis: Secret Sharing Schemes with Application in Security Protocols
    b. Institute: “Al.I.Cuza” University of Iasi
    c. Date: January 2007
    d. Degree: “Cum Laude” degree
- Catalin Birjoveanu
    a. PhD Thesis: Secrecy for Security Protocols
    b. Institute: “Al.I.Cuza” University of Iasi
    c. Date: January 2007

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

1. Adrian Schipor (2012-2016)
2. Raluca Chirosca (2012-2016)
3. Mihai Barzu (2011-2012)
4. Sonia Bogos, Loredana Vamanu, Constantin Dragan (2010)

5. Raluca Diaconu (2009)
6. Elena Badarau (2008)
7. Ioana Boureanu (2007)
8. Elena Erbiceanu (June 2005)
9. Claudia Prajescu, Razvan Zlavog (June 2004)
10. Constantin Enea, Dragos Trinca, Bogdan Pasaniuc, Ionut Popa (June 2003)
11. Bernard Ciurariu, Roxana Melinte, Ioana Olga, Olivia Onea (June 2002)
12. Cristina Badarau, Corina Apachite (September 2001)
13. Sorin Iftene (June 2000)
14. Cristian Ioan (February 1999)
15. Hollo Csaba (June 1996)
16. 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 National Council for the Attestation of University Titles, Diplomas and Certificates (2017 –)
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 National Council for the Attestation of University Titles, Diplomas and Certificates (2011 - 2013)
4. Member of the National University Research Council of Romania (2005 – 2009)

Departmental Activities:

1. Committee on Tenure Appointments (1997, 2000, 2001, 2002, 2003, 2007, 2009, 2010, 2012, 2013)
2. Committee on M.S. Programs (1998, 2000, 2001, 2006, 2007, 2008,2012)
3. Committee on Ph.D. Programs (1998, 2000, 2001, 2002, 2003, 2004, 2006, 2007, 2008, 2011, 2013)

Professional Activities:

1. Program Committees
   - (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 "Al.I.Cuza" University of Iasi, Computer Science Section (until 2007)
3. Editor
   - Scientific Annals of the "Al.I.Cuza" University of Iasi, Computer Science Section
4. Journal Referee
   - Acta Informatica, Fundamenta Informaticae, Information Processing Letters, Theoretical Computer Science, Acta Cybernetica, IEEE Journal on Computing, IEEE transactions on Computers, IEEE Transactions on Systems, Man and Cybernetics, 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 Conference on Mathematical Foundations of Informatics, July 2 – 6, 2018, Chisinau, Republic of Moldova (talk: Multi-linear Maps in Cryptography).
2. 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).
3. 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).
4. 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).

5. 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).
6. 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).
7. Invited talk at the Workshop on Circuits, Systems and Information Technology, WCSIT 2014 (talk: The way to modern cryptography).
8. 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).
9. 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).
10. 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/.
11. Invited Professor at the Doctoral School of LACL, Univ. Paris 12 (September 2008), http://lacl.univ-paris12.fr/.
12. Invited talk at the NATO Advanced Research Workshop on Information Security in Wireless Networks (September 4-8, 2006, Suceava, Romania), http://iwiswn.usv.ro/.
13. Invited talk at VERIMAG (Grenoble, France) on *Abstractions of Data Types*, July 11, 2005, http://www-verimag.imag.fr/SEMINAIRES/05/.
14. 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.
15. Invited talk at University of Central Florida, School of Computer Science, on *Abstraction Techniques for Program Analysis*, Sept 24, 2004.
16. Invited talk at University of Central Florida, School of Computer Science, on *Modeling and Verification of Security Protocols*, June 28, 2004.
17. SVC talk at Carnegie-Mellon University on *Abstractions of Data Types*, Pittsburgh (USA), May 4, 2004, http://www-2.cs.cmu.edu/~svc/.
18. Invited talk at the NATO Advanced Research Workshop *Concurrent Information Processing and Computing CIPC 2003*, Sinaia (Romania), July 5-10, 2003.
19. Invited talk at the *Austrian Workshop on Computer-Aided Verification of Information Systems CAVIS 2003*, Timisoara (Romania), 2003.
20. Invited talk at Carnegie-Mellon University, January 2001 and October 2001.
21. Invited talk at Jozsef Attila University of Szeged on *Petri Net Reactive Modules*, Szeged (Hungary), 2001.
22. Advanced research seminar on *Petri Nets*, Augsburg (Germany), Nov 1999 - Feb 2000.

23. Invited talk at Katholische Universitaet Eichstaett-Ingolstadt, Eichstaett (Germany), 1999
24. Invited talk and lectures at Kyoto Sangyo University, Kyoto (Japan), 1996 .
25. Invited talk at the *Symposium on Semigroups, Languages and Related Fields*, Shimane University (Japan), 1995.
26. Invited talk at the *Workshop on Semigroups, Formal Languages and Computer Systems*, Kyoto Sangyo University, Kyoto (Japan), 1995.
27. Invited talk at Freiburg University, Freiburg (Germany), 1995.

Publications

Books:

1. F.L. Tiplea: Algebraic Foundations of Computer Science, Editura Polirom, 2006 (581+xiii pages).
2. T. Jucan, F.L. Tiplea: Petri Nets. Theorie and Application, Romania Academy Publishing House, Bucharest, 1999 (238+x pages).
3. F.L. Tiplea: Introduction to Set Theory, "Al.I.Cuza" University Publishing House, Iasi, 1998 (306 + xiv pages).
4. T. Jucan, F.L. Tiplea: Petri Nets, "Al.I.Cuza" University Publishing House, 1995 (200 pages).

Edited Volumes:

1. C. Dima, M. Minea, F.L. Tiplea (eds.): Proceedings of the 1st International Workshop on Information and Computer Security ICS 2006, Timisoara (Romania), Sept 2006, ENTCS 186, 2007.
2. E. Clarke, M. Minea, F.L. Tiplea (eds.): Proceedings of the NATO Advanced Research Workshop *Verification of Infinite-state Systems with Applications to Security VISSAS 2005*, IOS Press, 2006.
3. D. Grigoras, A. Nicolau, F.L. Tiplea (eds.): Proceedings of the NATO Advanced Research Workshop “Concurrent Information Processing and Computing” CIPC2003, Sinaia (Romania), July 5-10, 2003.
4. T. Jucan, F.L. Tiplea (eds.): Proceedings of the 11th Romanian Symposium on Computer Science ROSYCS'98, Iasi (Romania), May 28- 30, 1998.

5. T. Jucan, H. Luchian, C. Masalagiu, F.L. Tiplea (eds.): Proceedings of the 10th Romanian Symposium on Computer Science ROSYCS'96, Iasi (Romania), May 30- June 1, 1996.

Refereed Contributions to Edited Volumes:

1. F.L. Tiplea, C. Birjoveanu, C. Enea: Complexity of the Secrecy Problem for Bounded Security Protocols, Proceedings of the NATO Advanced Research Workshop on Information Security for Wireless Networks, IOS Press 2007.
2. F.L. Tiplea, C. Enea, C. Birjoveanu: Decidability and Complexity Results for Security Protocols, Proceedings of the NATO Advanced Research Workshop *Verification of Infinite-state Systems with Applications to Security VISSAS 2005*, IOS Press 2006, 185-211.
3. F.L. Tiplea, A. Tiplea: A Compositional Semantics for Petri Net Reactive Modules, Proceedings of the NATO Advanced Research Workshop "Concurrent Information Processing and Computing" CIPC2003 (D. Grigoras, A. Nicolau, eds.), Sinaia (Romania), vol. 195 NATO Science Series "Computer and Systems Sciences", IOS Press, March 2005.
4. F.L. Tiplea, O. Procopiuc, C.M. Procopiuc, C. Ene: On the Power and Complexity of Parallel Communicating Grammar Systems, in: Artificial Life. Grammatical Models (A. Salomaa, Gh. Paun, eds.), The Black See University Publishing House, 1994.
5. F.L. Tiplea, T. Jucan: Jumping Petri Nets, in: Mathematical Linguistics and Related Topics (Gh. Paun, ed.), Romanian Academy Publishing House, Bucharest, 1994, 330-341.
6. F.L. Tiplea: On Conditional Grammars and Conditional Petri Nets, in: Mathematical Aspects of Natural and Formal Languages (Gh. Paun, ed.), World Scientific, Singapore, 1994, 431-456.

Papers Published in Refereed Journals:

1. F.L. Tiplea, C. Varlan: Group Anonymity in Security Protocols, Information Sciences (submitted).
2. C. Dragan, F.L. Tiplea: On the Asymptotic Idealness of the Asmuth-Bloom Threshold Secret Sharing Scheme, Information Sciences (to appear).
3. C. Dragan, F.L. Tiplea: Distributive Weighted Threshold Secret Sharing Schemes, *Information Sciences*, 339, 85-97, January 2016.

4. F.L. Tiplea, I. Leahu: The Reversible Released Form of Petri Nets and Its Applications to Soundness of Workflow Nets, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Feb 2016, vol 46(2), 303-312.
5. F.L. Tiplea, C. Bocaneala, R. Chirosca: On the Complexity of Deciding Soundness of Acyclic Workflow Nets, *IEEE Transactions on SMC: Systems*, 45(9), 1292-1298, March 2015.
6. F.L. Tiplea, R. Diaconu: Petri Net Computers and Workflow Nets, *IEEE Transactions on SMC: Systems*, 45(3), 498-507, August 2014.
7. F.L. Tiplea, C.C. Dragan: A Necessary and Sufficient Condition for the Asymptotic Idealness of the GRS Threshold Secret Sharing Scheme, *Information Processing Letters*, 114, 299-303, 2014.
8. M. Barzu, F.L. Tiplea, C.C. Dragan: Compact Sequences of co-primes and their Applications to the Security of CRT-based Threshold Schemes, *Information Sciences*, vol. 240, 2013, 161-172.
9. F.L. Tiplea, C. Bocaneala: Priority Workflow Nets, *IEEE Transactions on Systems, Man and Cybernetics: Systems*, vol. 43(2), 2013, 402-415.
10. F.L. Tiplea, C. Bocaneala: Resource Relocation in Workflow Nets with Time, Resource, and Task Priority Constraints, *IEEE Transactions on Systems, Man and Cybernetics: Systems*, vol 44, issue 7, 953-965, 2014.
11. F.L. Tiplea, L. Vamanu, C. Varlan: Reasoning about Minimal Anonymity in Security Protocols, *Future Generation Computer Systems* (Elsevier), 29(3), 2013, 828-842.
12. F.L. Tiplea, C. Bocaneala: Decidability Results for Soundness Criteria of Resource-constrained Workflow Nets, *IEEE Transactions on Systems, Man and Cybernetics (Part A: Systems and Humans)*, vol. 42(1), 2012, 238-249.
13. F.L. Tiplea, G. Macovei: Soundness for S- and A-Timed Workflow Nets is Undecidable, *IEEE Transactions on Systems, Man and Cybernetics (Part A: Systems and Humans)*, vol. 39(4), July 2009, 924-932.
14. F.L. Tiplea, C. Birjoveanu, C. Enea, I. Boureanu: Secrecy for Bounded Protocols With Freshness Check is NEXPTIME-complete, *Journal of Computer Security*, vol. 16, no. 6, 689-712, 2008.
15. F.L. Tiplea, A. Tiplea: Petri Net Reactive Modules, *Theoretical Computer Science* 359, 2006, 77-100.
16. F.L. Tiplea, C. Enea: Abstractions of Data Types, *Acta Informatica* 42(8-9), 2006, 639-671.
17. F.L. Tiplea, D.C. Marinescu: Structural Soundness for Workflow Nets is Decidable, *Information Processing Letters* 96, 2005, 54-58.
18. F.L. Tiplea, E. Mäkinen, D. Trinca, C. Enea: Characterization Results for Time-Varying Codes, *Fundamenta Informaticae* 52, 2002, 1-13.

19. R. Melinte, O. Oanea, I. Olga, F.L. Tiplea: The Home Marking Problem and Some Related Concepts, *Acta Cybernetica* 15(3), 2002.
20. F.L. Tiplea, E. Mäkinen: On the Complexity of a Problem on Monadic String Rewriting Systems, *Journal of Automata, Languages and Combinatorics* 7(4), 2002, 599-609.
21. F.L. Tiplea, E. Mäkinen, C. Enea: SE-Systems, Timing Mechanisms, and Time-Varying Codes, *International Journal of Computer Mathematics* 79(10), 2002, 1083-1091.
22. F.L. Tiplea, E. Mäkinen: A Note on SE-systems and Regular Canonical Systems, *Fundamenta Informaticae* 46, 3 (2001), 253-256.
23. F.L. Tiplea, E. Mäkinen: A Note on Synchronized Extension Systems, *Information Processing Letters* 79, 2001, 7-9.
24. F.L. Tiplea, E. Mäkinen, C. Apachite: Syncronized Extension Systems, *Acta Informatica* 37, 2001, 449-465.
25. F.L. Tiplea, C. Badarau: A Note on Decidability of Reachability for Conditional Petri Nets, *Acta Cybernetica* 14, 2000, 455-459.
26. F.L. Tiplea, A. Tiplea: On Normalization of Petri Nets, *Scientific Annals of the ``Al.I.Cuza'' University of Iasi*, Computer Science Section, Tome VIII, 1999, 151-161.
27. F.L. Tiplea, E. Mäkinen: Jumping Petri Nets. Specific Properties, *Fundamenta Informaticae* 32, 1997, 373-392.
28. E. Mäkinen, F.L. Tiplea: Pattern Preserving Ambiguities for Pure Context-Free Grammars, *Fundamenta Informaticae* 30, 1997, 183-191.
29. F.L. Tiplea, M. Katsura, M. Ito: Processes and Vectorial Characterizations of Parallel Communicating Grammar Systems, *Journal of Automata, Languages and Combinatorics* 2, 1997, 47-73.
30. F.L. Tiplea, M. Katsura, M. Ito: On a Normal Form of Petri Nets, *Acta Cybernetica* 12, 1996, 295-308.
31. F.L. Tiplea, G. Macovei: Selective Grammars, *Annals of the University of Bucharest*, Ser. Math.-Inform. 1995, 61-68.
32. F.L. Tiplea, C. Ene: Hierarchies of Petri Net Languages and a Super-Normal Form, *Journal of Automata, Languages and Combinatorics* 2, 1997, 187-204.
33. F.L. Tiplea, C. Ene, C.M. Ionescu, O. Procopiuc: Some Decision Problems for Parallel Communicating Grammar Systems, *Theoretical Computer Science* 134, 1994, 365-385.
34. F.L. Tiplea, T. Jucan: Jumping Petri Nets, Foundations of Computing and Decision Sciences 19, no. 4, 1994, 319-332.
35. C.M. Ionescu, O. Procopiuc, F.L. Tiplea: Parallel Communicating Grammar Systems: the Context-Sensitive Case, *International Journal of Computer Mathematics* 49, no. 3-4, 1993, 145-156.

36. F.L. Tiplea, C. Ene: A Coverability Structure for Parallel Communicating Grammar Systems, *Journal of Information Processing and Cybernetics* EIK 29, no. 5, 1993, 303-315.
37. F.L. Tiplea, T. Jucan, C. Masalagiu: Relation Based Controlled Petri Nets, *Scientific Annals of the "Al.I.Cuza" University of Iasi*, Section Inf. 1, 1993.
38. F.L. Tiplea: Selective Petri Net Languages, *International Journal of Computer Mathematics* 43, no.1+2, 1992, 61-80.
39. F.L. Tiplea: On Place Restricted Petri Nets, *Foundation of Computing and Decision Sciences* 16, no.1, 1991, 29-38.
40. F.L. Tiplea, T. Jucan, C. Masalagiu: Conditional Petri Net Languages, *Journal of Information Processing and Cybernetics* EIK 27, no.1, 1991, 55-66.
41. C. Masalagiu, T. Jucan, F.L. Tiplea: A Refinement of the Matching Extension Operations, *Scientific Annals of the ``Al.I.Cuza'' University of Iasi*, Section Math.-Inf. 35, no.4, 1989, 343-351.
42. F.L. Tiplea, T. Jucan, C. Masalagiu: Matching Extensions for Petri Net Languages, *Scientific Annals of the ``Al.I.Cuza'' University of Iasi*, Section Math.-Inf. 35, no.4, 1989, 337-342.
43. F.L. Tiplea: Reversible and Strict Reversible P/T-Systems, *Scientific Annals of the ``Al.I.Cuza'' University of Iasi*, Section Math.-Inf. 34, no.4, 1988, 319-327.
44. F.L. Tiplea, T. Jucan, C. Masalagiu: Term Rewriting Systems and P/T-Nets, *Scientific Annals of the "Al.I.Cuza" University of Iasi*, Section Math.-Inf. 34, no.4, 1988, 305-317.
45. T. Jucan, C. Masalagiu, F.L. Tiplea: Sufficient Conditions for the Decidability of s->*t, *Scientific Annals of the ``Al.I.Cuza'' University of Iasi*, Section Math.-Inf. 34, no. 4, 1988, 295-303.
46. F.L. Tiplea: On General Unification, *Mathematical Reports* 40, no. 2, 1988, 161-172.

Papers Presented at Refereed Conferences:

1. F.L. Tiplea, C. Dragan, A.-M. Nica: Key-Policy Attribute-Based Encryption from Bilinear Maps, 10th International Conference SECITC 2017, LNCS 10543, 28-42, 2017.
2. F.L. Tiplea, S. Iftene, G. Teseleanu, A.-M. Nica: Security of Identity-based Encryption Schemes from Quadratic Residuosity, 9th International Conference SECITC, 9-10 June 2016, LNCS 10006, 63-74.
3. C. Dragan, F.L. Tiplea: Key-Policy Attribute-Based Encryption for General Boolean Circuits from Secret Sharing and Multi-linear Maps, Second International Conference, BalkanCryptSec 2015, Koper, Slovenia, September 3-4, 2015 (Revised selected papers:

Cryptography and Information Security in the Balkans, volume 9540 of the series Lecture Notes in Computer Science pp 112-133, Jan 2016).

4. F.L. Tiplea, E. Simion: New Results on IBE from Quadratic Residuosity, 8th International Conference SECITC 2015, Bucharest, Romania, June 11-12, 2015.
5. G.D. Nastase, F.L. Tiplea: On a lightweight authentication protocol for RFID, 8th International Conference SECITC 2015, Bucharest, Romania, June 11-12, 2015 (Revised selected papers: Innovative Security Solutions for Information Technology and Communications, volume 9522 of the series Lecture Notes in Computer Science, pp 212-225, 2015).
6. F.L. Tiplea, C. Dragan: Key-policy Attribute-based Encryption for Boolean Circuits from Bilinear Maps, First International Conference BalkanCryptSec 2014, Istanbul, Turkey, October 16-17, 2014 (Revised selected papers: Cryptography and Information Security in the Balkans, volume 9024 of the series Lecture Notes in Computer Science pp 175-193, July 2015).
7. F.L. Tiplea: A lightweight authentication protocol for RFID, Third International Conference, CSS 2014, Lublin, Poland, September 22-24, 2014 (Cryptography and Security Systems, volume 448 of the series Communications in Computer and Information Science pp 110-121, 2014).
8. F.L. Tiplea: The way to modern cryptography, Workshop on Circuits, Systems and Information Technology, WCSIT 2014.
9. F.L. Tiplea: Identity-based Encryption, Romanian Cryptology Days, 2013
10. F.L. Tiplea: Modeling and Analysis of Security Protocols, Romanian Cryptology Days, 2011.
11. C. Dima, C. Enea, D. Guelev, F.L. Tiplea: Positive and Negative Results on the Model-checking Problem for ATL with Imperfect Information, 2nd Workshop on Games for Design, Verification, and Synthesis (collocated with CONCUR 2010), Paris, France, Sept. 2010.
12. F.L. Tiplea, L. Vamanu, C. Varlan: Complexity of Anonymity for Security Protocols, 15th European Symposium on Computer Science ESORICS 2010, Sept 20-22, Athens (Greece), Lecture Notes in Computer Science 6345, 2010, 558-572.
13. L. Cojocaru, E. Makinen and F. L. Tiplea: Classes of Szilard Languages in NC1, in "*Advances in the Theory of Computing"* (AITC'09), special track of the 11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2009), 2009, IEEE Computer Society Press, 299-306.
14. F. Hamza-Lup, F.L. Tiplea: An Automaton-based Formalism for Cooperative Augmented Reality Systems, Workshop on Non-classical Models for Automata and Applications (NCMA), Wroclaw (Poland), 2009, Austrian Computer Society, 135-150.

15. F.L. Tiplea, C. Birjoveanu, C. Enea: Complexity of the Secrecy Problem for Bounded Security Protocols, NATO Advanced Research Workshop on Information Security for Wireless Networks, IOS Press 2006, 185-211.
16. F.L. Tiplea, G. Macovei: E-Timed Workflow Nets, Proc. of the 8th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, September 26 - 29, 2006, IEEE Computer Society Press, 423-429 (DOI 10.1109/SYNASC.2006.33).
17. I. Leahu, F.L. Tiplea: The Confluence Property for Petri Nets and its Applications, Proc. of the 8th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, September 26 - 29, 2006, IEEE Computer Society Press, 430-436 (DOI 10.1109/SYNASC.2006.71).
18. F.L. Tiplea, A. Tiplea: Instantiating Nets with Applications to Workflow Nets, Proc. of the 7th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, September 25 - 29, 2005, IEEE Computer Society Press, 367-373.
19. F.L. Tiplea, G. Macovei: Timed Workflow Nets, Proc. of the 7th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, September 25 - 29, 2005, IEEE Computer Society Press, 361-366.
20. F.L. Tiplea, C. Enea, C. Birjoveanu: Decidability and Complexity Results for Security Protocols, NATO Advanced Research Workshop *Verification of Infinite-state Systems with Applications to Security VISSAS 2005*, Timisoara (Romania), March 17-22, 2005, IOS Press 2006, 185-211.
21. F.L. Tiplea, D.C. Marinescu, C. Lin: Model Checking and Abstraction for Workflow Net Verification, 1st International Workshop on Coordination and Petri Nets, Bologna (Italy), June 21, 2004, 131-145.
22. F.L. Tiplea, O. Oanea: Model Checking Linear Time mu-Calculus for Extended Petri Nets, 5th International Workshop "Symbolic and Numeric Algorithms for Scientific Computing" SYNASC 2003, Timisoara (Romania), Oct 1-4, 2003, 297-310.
23. F.L. Tiplea, A. Tiplea: A Compositional Semantics for Petri Net Reactive Modules, NATO Advanced Research Workshop CIPC2003, Sinaia (Romania), IOS Press, 2004 (to appear).
24. R. Melinte, O. Oanea, I. Olga, F.L. Tiplea: The Home Marking Problem and Some Related Concepts, PROMISE 2002, Potsdam (Germany), 2002, Lecture Notes in Informatics, 104-115.
25. F.L. Tiplea, A. Tiplea: A Simulation Preorder for Abstraction of Reactive Systems, Third Workshop on "Verification, Model Checking and Abstract Interpretation" VMCAI02, Venice (Italy), January 21-22, 2002, Lecture Notes in Computer Science 2294, 272-288.

26. F.L. Tiplea, E. Mäkinen: On the Complexity of a Problem on Monadic String Rewriting Systems, Third Workshop on ``Descriptional Complexity of Automata, Grammars and Related Structures", Vienna (Austria), July 20-22, 2001.
27. F.L. Tiplea, J. Desel: Petri Net Process Decomposition with Application to Validation, Procc. of the 6th Conference on Algorithms and Tools for Petri Nets, Frankfurt am Main (Germany), Oct 11-12, 1999.
28. F.L. Tiplea, A. Tiplea: On Normalization of Petri Nets, Proc. of the 11th Romanian Symposium on Computer Science ROSYCS'98, Iasi (Romania), May 1998.
29. F.L. Tiplea, E. Mäkinen: Jumping Petri Nets. Specific Properties, Proc. of the the 3rd International Conference ``Developments in Language Theory", Thessaloniki (Greece), 1997.
30. F.L. Tiplea, T. Jucan: Complexity of Petri Nets, Proc. of the 10th Romanian Symposium on Computer Science ROSYCS'96, Iasi (Romania), May 1996, 1-26.
31. F.L. Tiplea, T. Jucan: Petri Net Languages, Proc. of the 10th Romanian Symposium on Computer Science ROSYCS'96, Iasi (Romania), May 1996, 71-96.
32. F.L. Tiplea: On Computational Power of Jumping Petri Nets, Proc. of the Workshop on Semigroups, Formal Languages and Computer Systems, RIMS Kokyuroku 960, Kyoto (Japan), 1996, 165-177.
33. F.L. Tiplea, M. Katsura, M. Ito: On Replacement of Petri Nets and Some Applications, Proc. of the Workshop on Semigroups, Formal Languages and Computer Systems, RIMS Kokyuroku 960, Kyoto (Japan), 1996, 178-190.
34. F.L. Tiplea: Petri Net Languages, Proc. of the 19th Symposium on Semigroups, Languages and their Related Fields, Shimane (Japan), 1995, 71-86.
35. C. Matei, F.L. Tiplea: (0,1)-Total Pure Context-Free Grammars, Proc. of the 2nd International Conference "Developments in Language Theory", Magdeburg, Germany, 1995, 148-153.
36. F.L. Tiplea, C. Ene: Hierarchies of Petri Net Languages and a Super-Normal Form, Proc. of the 2nd International Conference "Developments in Language Theory", Magdeburg (Germany), 1995, 396-408.
37. F.L. Tiplea: Jumping Petri Nets, 7th International Conference on Automata and Formal Languages, Salgotarjan (Hungary), 1993.
38. F.L. Tiplea, T.Jucan, St.Dumbrava: Modeling Systems by Petri Nets with Different Degrees of Concurrency, Proc. of the 14th International Symposium on Automatic Control and Computer Science SACCS'93, Iasi (Romania), 1993, 48-54.
39. F.L. Tiplea: New Remarks on Conditional Grammars and Conditional Petri Nets, Proc. of the 8th Symposium on Computer Science INFO-IASI, Iasi (Romania), Nov 14 - 16, 1991.

40. C. Masalagiu, T. Jucan, F.L. Tiplea: A Refinement of the Matching Extension Operations, Proc. of the 7th Symposium on Computer Science INFO-IASI, Iasi (Romania), Oct 19 - 21, 1989, 110-116.
41. F.L. Tiplea, T. Jucan, C. Masalagiu: Conditional Petri Net Languages, Proc. of the 7th Symposium on Computer Science INFO-IASI, Iasi (Romania), Oct 19 - 21, 1989, 110-116.
42. F.L. Tiplea, T. Jucan, C. Masalagiu: Matching Extensions for Petri Net Languages, Proc. of the 7th Symposium on Computer Science INFO-IASI, Iasi (Romania), Oct 19 - 21, 1989, 151-155.
43. F.L. Tiplea: Almost Regular ACFM Theories, Proc. of the 6th Symposium on Computer Science INFO-IASI, Iasi (Romania), Oct 9 - 10, 1987, 192-201.

Technical Reports:

1. F.L. Tiplea, C. Dragan : Key-policy Attribute-based Encryption for Boolean Circuits from Bilinear Maps, Cryptology ePrint Archive, Report 2014/608, 2014, http://eprint.iacr.org/.
1. C.C Dragan and F.L. Tiplea : Effcient key-policy attribute-based encryption for general Boolean circuits from multi-linear maps. Cryptology ePrint Archive, Report 2014/462, 2014, http://eprint.iacr.org/.
2. F. Hamza-Lup, F.L. Tiplea: An Automata-based Formalism for Cooperative Augmented Reality Systems, IEEE Transactions on Modeling and Computer Simulation (submitted).
3. F.L. Tiplea, C. Enea, C. Birjoveanu: Decidability and Complexity Results for Security Protocols, Technical Report TR 05-02, “Al.I.Cuza” University of Iasi, June 2005.
4. F.L. Tiplea, S. Iftene, C. Hritcu, I. Goriac, R.M. Gordan, E. Erbiceanu: MpNT: A Multi-Precision Number Theory Package. Number-Theoretic Algorithms (I), Technical Report TR 03-02, Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania, May 2003.
5. R. Melinte, O. Oanea, I. Olga, F.L. Tiplea: The Home Marking Problem and Some Related Concepts, Technical Report 02-02, Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania, February 2002.
6. F.L. Tiplea, S. Iftene, B. Ciurariu, C. Apachi tei: Subset Based Properties of Partially Ordered Sets, Technical Report 02-02, Faculty of Computer Science, "Al.I.Cuza" University of Iasi, Romania, February 2002.
7. F.L. Tiplea, E. Mäkinen: On the Complexity of a Problem on Monadic String Rewriting Systems, Technical Report A-2001-4, Department of Computer and Information Sciences, University of Tampere, Finland, June 2001.

8. F.L. Tiplea, E. Mäkinen, C. Enea: SE-Systems, Timing Mechanisms, and Time-Varying Codes, Technical Report A-2000-17, Department of Computer and Information Sciences, University of Tampere, Finland, December 2000.
9. F.L. Tiplea, E. Mäkinen: On SE-Systems and Monadic String Rewriting Systems, Technical Report A-2000-15, Department of Computer and Information Sciences, University of Tampere, Finland, November 2000.
10. F.L. Tiplea, E. Mäkinen: A Note on SE-systems and Regular Canonical Systems, Technical Report A-2000-14, Department of Computer and Information Sciences, University of Tampere, Finland, October 2000.
11. F.L. Tiplea, E. Mäkinen: A Note on Syncronized Extension Systems, Technical Report A-2000-11, Department of Computer and Information Sciences, University of Tampere, Finland, July 2000.
12. F.L. Tiplea, E. Mäkinen, C. Apachite: Syncronized Extension Systems, Technical Report A-2000-1, Department of Computer and Information Sciences, University of Tampere, Finland, January 2000, 19 pp.
13. F.L. Tiplea, A. Tiplea: Petri Net Reactive Modules, Technical Report 1999-7, Institut fur Informatik, Universität Augsburg, Dec 1999, 50 p.
14. F.L. Tiplea, E. Mäkinen: Jumping Petri Nets. Specific Properties, Technical Report A-1996-8, Department of Computer Science, University of Tampere, Tampere (Finland), 1996.
15. E. Mäkinen, F.L. Tiplea: Pattern Preserving Ambiguities for Pure Context-Free Grammars, Technical Report A-1996-6, Dept. of Computer Science, University of Tampere, Tampere (Finland), 1996.

April 29, 2018

Prof.dr. Ferucio Laurentiu Tiplea