Ferucio Laurențiu ȚIPLEA, Ph.D.

Professor
Department of Computer Science
"Alexandru Ioan Cuza" University of Iași
Iași 700506, Romania
Tel: +40-(0)742-019593
E-mail: ferucio.tiplea@uaic.ro
URL: https://www.flt-info.eu

Education

1. April 1993: Ph.D., Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania. Thesis on *Petri Nets*;
2. June 1986: BSc, Mathematics, Computer Science Section (four-year study program), "Alexandru Ioan Cuza" University of Iași, Romania. Thesis on *Unification Algorithms in Equational Theories*.

Research Interests

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

Academic Positions

1. July 2000 – present: Ph.D. supervisor (OMEN no. 4211/20.07.2000);
2. Nov 1999 – present: Professor, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania;
3. Oct 1995 – Nov 1999: Associate Professor, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania;
4. Feb 1992 – Oct 1995: Lecturer, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania;
5. July 1991 – Feb 1992: Assistant Professor, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania;
6. Oct 1990 – July 1991: Assistant Professor, Department of Mathematics, "Alexandru Ioan Cuza" University of Iași, Romania.

Other Positions

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

Visiting Appointments

1. Sept 2008: Visiting Professor, LACL, Université Paris 12 Val de Marne, Créteil, France;
2. Dec 21, 2003 – May 6, 2006: Visiting Professor, School of Computer Science, University of Central Florida, Florida, USA;
3. Oct 1 - Nov 30, 2001: Visiting Scientist, Department of Computer Science, Carnegie Mellon University, Pittsburg, Pennsylvania, USA;
4. January 15 - April 14, 2001: Fulbright Fellow, Department of Computer Science, Carnegie Mellon University, Pittsburg, Pennsylvania, USA;
5. September 20, 1999 - March 20, 2000: German Academy Fellow, Institut für Informatik, Universität Augsburg, Germany;
6. June 30 - August 30, 1999: DAAD Fellow, Institut für Informatik, Universität Eichstädt, Germany;
7. October 1995 - March 1997: Monbusho Fellow, Department of Computer Science, Kyoto Sangyo University, Japan;
8. May 1 – July 31, 1995: DAAD Fellow, Institute für Informatik, Universität Freiburg, Germany.

Teaching Experience

Throughout my career, I have been involved in a wide variety of courses or seminar activities:

1. Network Security: Graduate course, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania, since 2010;
2. Algebraic Foundations of Computer Science: Undergraduate course, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania, since 1994;
3. Information Security: Undergraduate course, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania, since 2008;
4. Decidability and Complexity: Undergraduate course, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania, since 1992;
5. Introduction to Cryptography (formerly, Coding Theory and Cryptography): Undergraduate course, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania, since 1994;

6. Security Protocols: Graduate course, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania (Spring 2000, 2001; Fall 2002; Spring 2005 – 2007);
7. Verification Techniques for Security Protocols: Graduate course, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania, Fall 2006 – 2008;
8. Introduction to Discrete Structures COT3100H: Honors course, School of Computer Science, University of Central Florida (The Burnett Honors College), Spring 2006;
9. Formal Languages and Automata COT5310: Graduate course, School of Computer Science, University of Central Florida (Spring 2005; Fall 2005);
10. Program Analysis COP5021: Graduate course, School of Computer Science, University of Central Florida (Fall 2004; Spring 2006);
11. Program Analysis: Ph.D. course, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania (Fall 2005; Spring 2008, 2009). In Sept 2008, I taught this course at LACL, Université Paris 12 Val de Marne, France;
12. Numerical Calculus COT4500: Undergraduate course, School of Computer Science, University of Central Florida (Spring 2004);
13. Petri Nets: Graduate seminar (with Prof.dr. Walter Vogler), Institut für Informatik, Universität Augsburg, Germany (Fall 1999);
14. Distributed Systems: Modeling and Analysis with Petri Nets: Graduate course, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania (Spring 1997, 1998, 1999);
15. Introduction to Computer Science: Undergraduate course, Faculty of Sociology, "Alexandru Ioan Cuza" University of Iași, Romania (Fall 1992, 1993, 1994);
16. Logic Programming: Undergraduate seminars/labs, Department of Computer Science, "Alexandru Ioan Cuza" University of Iași, Romania (Spring 1991, 1992, 1993, 1994).

Ph.D. Students[1]

- Current Ph.D. Students:
  1. Simona Lăzărescu (since Fall 2023)
     - Main topic: lattice-based cryptography
  2. Olimpia Țicloș (since Fall 2022)
     - Main topic: lattice-based cryptography
  3. Paul Cotan (since Fall 2021)
     - Main topic: higher-order residues in cryptography
  4. Cristian Hristea (since Fall 2016)
     - Main topic: security and privacy of RFID protocols
- Former Ph.D. Students:
  1. George Teșeleanu

[1] I have supervised Ph.D. students since 2000 because Romanian legislation allowed obtaining the title of doctoral supervisor only after receiving the title of full professor.

- Ph.D. Thesis: Cryptographic Protocols
- Institute: “Simion Stoilow” Institute of Mathematics of the Romanian Academy
- Date: Oct 2021

2. Cătălin Liță
   - Ph.D. Thesis: Malware Detection and Analysis
   - Institute: “Alexandru Ioan Cuza” of Iași, Romania
   - Date: Oct 2018
3. Iulian Goriac
   - Ph.D. Thesis: An Epistemic Logic Based Framework for Reasoning about Information Hiding
   - Institute: “Alexandru Ioan Cuza” University of Iași
   - Date: March 2015
4. Cătălin Drăgan
   - Ph.D. Thesis: Security of the CRT-based Secret Sharing Schemes
   - Institute: “Alexandru Ioan Cuza” University of Iași
   - Date: September 2013
5. Cosmin Vârlan
   - Ph.D. Thesis: Anonymity in Security Protocols
   - Institute: “Alexandru Ioan Cuza” University of Iași
   - Date: April 2013
6. Corina Dima (married Bocăneală)
   - Ph.D. Thesis: Workflow Nets with Time, Resource, and Priority Constraints
   - Institute: “Alexandru Ioan Cuza” University of Iași
   - Date: March 2013
7. Mogoș Gabriela
   - Ph.D. Thesis: Quantum Cryptography
   - Institute: “Alexandru Ioan Cuza” University of Iași
   - Date: January 2010
8. Constantin Enea
   - Ph.D. Thesis: Verification by Abstraction
   - Institute: Univ. Paris 12 Val de Marne
   - Date: January 2008
   - Degree: “Tres Honorable”
9. Geanina Macovei
   - Ph.D. Thesis: Timed Petri Nets and Workflow Nets
   - Institute: “Alexandru Ioan Cuza” University of Iași
   - Date: January 2008
10. Sorin Iftene

- Ph.D. Thesis: Secret Sharing Schemes with Application in Security Protocols
- Institute: "Alexandru Ioan Cuza" University of Iași
- Date: January 2007

11. Cătălin Bîrjoveanu
    - Ph.D. Thesis: Secrecy for Security Protocols
    - Institute: "Alexandru Ioan Cuza" University of Iași
    - Date: January 2007

Honor Students

Under my guidance, these students developed or strengthened their research skills, most of them publishing papers in specialized conferences or journals:

1. Denisa Țîflea, Rareș Radu, Alexandra Butnaru (ECCO 2022)
2. Alexandru Ioniță (SECRYPT 2020)
3. Diana Bolocan (RCD 2019)
4. Victor Pescaru (MFOI 2019)
5. Victor Talif (SECITC 2018)
6. Daniel Plecan (RCD 2017)
7. Lucian Oștepoc (SECITC 2016)
8. Adrian Schipor (BalkanCryptSec 2014, SECITC 2018)
9. Raluca Chiroșcă (IEEE SMCA 45(9), 2016)
10. Gabriel Năstase (SECITC 2015)
11. Mihai Barzu (Inf. Sciences 240, 2013)
12. Loredana Vamanu (FGCS 29(3), 2013)
13. Constantin Drăgan (SECRYPT 2009)
14. Raluca Diaconu (IEEE SMCA 45(3), 2015)
15. Ioana Boureanu (Journal of Computer Security 16(6), 2008)
16. Elena Erbiceanu (June 2005)
17. Claudia Prajescu, Razvan Zlavog (June 2004)
18. Constantin Enea, Dragos Trinca, Bogdan Pasaniuc, Ionut Popa (June 2003)
19. Bernard Ciurariu, Roxana Melinte, Ioana Olga, Olivia Onea (June 2002)
20. Corina Apachițe (September 2001, Acta Informatica)
21. Cristina Bădărău (Acta Cybernetica, 2000),
22. Sorin Iftene (June 2000)
23. Cristian Ioan (February 1999)
24. Hollo Csaba (June 1996)
25. Magdalena Ionescu, Octavian Procopiuc, Cristian Ene, Codruț Matei, Cristian Preda, Geanina Macovei (June 1995)

Contracts, Projects, and Grant Support

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

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. Păun (2012, 2014), L. Leuștean (2014), A. Popa (2017), C. Mureșan (2019), R. Olimid (2019), E. Simion (2021), C. Dima (2021).

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, 2021, 2022);
4. Committee on Ph.D. Programs (1998, 2000, 2001, 2002, 2003, 2004, 2006, 2007, 2008, 2011, 2012, 2013, 2015, 2018, 2020, 2021).

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, 2021, 2022;
    - 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, Iași, Romania, Sept 20-21, 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* (in conjunction with ECIT and ROSYCS), July 2002;
- Romanian Symposium on *Computer Science ROSYCS'98*, Iași (Romania), May 1998;
- Romanian Symposium on *Computer Science ROSYCS'96*, Iași (Romania), May 1996;

2. Managing Editor of Scientific Annals of the "Alexandru Ioan Cuza" University of Iași, Computer Science Section (until 2007);
3. Editor of Scientific Annals of the "Alexandru Ioan Cuza" University of Iași, Computer Science Section.

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. SVC talk at Carnegie-Mellon University on *Abstractions of Data Types*, Pittsburgh (USA), May 4, 2004, http://www-2.cs.cmu.edu/~svc/.
20. Invited talk at the NATO Advanced Research Workshop *Concurrent Information Processing and Computing CIPC 2003*, Sinaia (Romania), July 5-10, 2003.
21. Invited talk at the *Austrian Workshop on Computer-Aided Verification of Information Systems CAVIS 2003*, Timisoara (Romania), 2003.
22. Invited talk at Jozsef Attila University of Szeged on *Petri Net Reactive Modules*, Szeged (Hungary), 2001.

Books

1. F.L. Tiplea: Algebraic Foundations of Computer Science, second edition, revised and expanded: "Alexandru Ioan Cuza" University Publishing House, 2021 (605 pages, in Romanian). The first edition was published by Polirom Publishing House in 2006 (581+xiii pages, in Romanian).
2. T. Jucan, F.L. Tiplea: Petri Nets. Theory and Application, Romania Academy Publishing House, Bucharest, 1999 (238+x pages, in Romanian).
3. F.L. Tiplea: Introduction to Set Theory, "Alexandru Ioan Cuza" University Publishing House, Iași, 1998 (306 + xiv pages, in Romanian).
4. T. Jucan, F.L. Tiplea: Petri Nets, "Alexandru Ioan Cuza" University Publishing House, 1995 (189 + ix pages, in Romanian).

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, Iași (Romania), May 28- 30, 1998 (published as a special issue of "Analele Universității ”Al.I.Cuza” din Iași”, tom VIII, 1999).
5. T. Jucan, H. Luchian, C. Masalagiu, F.L. Tiplea (eds.): Proceedings of the 10th Romanian Symposium on Computer Science ROSYCS'96, Iași (Romania), May 30- June 1, 1996.

Refereed Contributions to Edited Volumes

1. F.L. Țiplea, C. Andriesei, C. Hristea: Security and Privacy of PUF-based RFID Systems, Chapter in ”*Cryptography - Recent Advances and Future Developments*”, IntechOpen, ISBN 978-1-83962-566-4, chapter published on Nov. 15th, 2020.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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 in Web of Science indexed journals with impact factor

All papers in this section are visible in Web of Science, ResearcherID B-9674-2011.

1. F.L. Ţtiplea: Efficient generation of roots of power residues modulo powers of two, *Mathematics*, vol 10(6), 908, 2022.
2. F.L. Țiplea: Lessons to be learned for a good design of private RFID schemes, *IEEE Transactions on Dependable and Secure Computing*, vol 19(4), 2022, 2384-2395.
3. F.L. Țiplea: Narrow privacy and desynchronization in Vaudenay’s RFID model, *International Journal of Information Security*, vol 21, 2022, 563-575.

4. F.L. Țiplea, C.C. Drăgan: Asymptotically ideal Chinese remainder theorem-based secret sharing schemes for multilevel and compartmented access structures, *IET Information Security*, vol. 15(4), 282-296, July 2021.
5. F.L. Țiplea, C. Hristea: PUF Protected Variables: A Solution to RFID Security and Privacy Under Corruption with Temporary State Disclosure, *IEEE Transactions on Information Forensics and Security*, vol. 16, 999-1013, 2021.
6. F.L. Țiplea, S. Iftene, G. Teșeleanu, A.-M. Nica: On the Distribution of Quadratic Residues and Non-residues Modulo Composite Integers and Applications to Cryptography, *Applied Mathematics and Computation*, vol. 372, May 2020.
7. C. Hristea, F.L. Țiplea: Privacy of Stateful RFID Systems With Constant Tag Identifiers, *IEEE Transactions on Information Forensics and Security*, vol. 15, 1920-1934, 2020.
8. C. Drăgan, F.L. Țiplea: On the Asymptotic Idealness of the Asmuth-Bloom Threshold Secret Sharing Scheme, *Information Sciences*, vol. 463–464, 75-85, Oct. 2018.
9. F.L. Țiplea, I. Leahu: The Reversible Released Form of Petri Nets and Its Applications to Soundness of Workflow Nets, *IEEE Transactions on SMC: Systems*, vol 46(2), 303-312, Feb. 2016.
10. C. Drăgan, F.L. Țiplea: Distributive Weighted Threshold Secret Sharing Schemes, *Information Sciences*, vol. 339, 85-97, April 2016.
11. F.L. Țiplea, C. Bocăneală, R. Chiroșcă: On the Complexity of Deciding Soundness of Acyclic Workflow Nets, *IEEE Transactions on SMC: Systems*, vol. 45(9), 1292-1298, March 2015.
12. F.L. Țiplea, R. Diaconu: Petri Net Computers and Workflow Nets, *IEEE Transactions on SMC: Systems*, vol. 45(3), 498-507, August 2015.
13. F.L. Țiplea, C. Bocăneală: Resource Relocation in Workflow Nets With Time, Resource, and Task Priority Constraints. *IEEE Transactions on SMC: Systems*, vol. 44(7), 953-965, July 2014.
14. F.L. Țiplea, C.C. Drăgan: A Necessary and Sufficient Condition for the Asymptotic Idealness of the GRS Threshold Secret Sharing Scheme, *Information Processing Letters*, vol. 114(6), 299-303, June 2014.
15. M. Barzu, F.L. Țiplea, C.C. Drăgan: Compact Sequences of co-primes and their Applications to the Security of CRT-based Threshold Schemes, *Information Sciences*, vol. 240, 161-172, Aug. 2013.
16. F.L. Țiplea, C. Bocăneală: Priority Workflow Nets, *IEEE Transactions on Systems, Man and Cybernetics: Systems*, vol. 43(2), 402-415, 2013.
17. F.L. Țiplea, L. Vamanu, C. Vârlan: Reasoning about Minimal Anonymity in Security Protocols, *Future Generation Computer Systems*, 29(3), 828-842, March 2013.
18. F.L. Țiplea, C. Bocăneală: 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), 238-249, 2012.

19. F.L. Țiplea, 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), 924-932, July 2009.
20. F.L. Țiplea, A. Țiplea: Petri Net Reactive Modules, *Theoretical Computer Science*, vol. 359, 77-100, 2006.
21. F.L. Țiplea, C. Enea: Abstractions of Data Types, *Acta Informatica*, vol. 42(8-9), 639-671, 2006.
22. F.L. Țiplea, D.C. Marinescu: Structural Soundness for Workflow Nets is Decidable, *Information Processing Letters*, vol. 96, 54-58, 2005.
23. F.L. Țiplea, E. Mäkinen, D. Trincă, C. Enea: Characterization Results for Time-Varying Codes, *Fundamenta Informaticae*, vol. 52, 1-13, 2002.
24. F.L. Țiplea, E. Mäkinen, C. Enea: SE-Systems, Timing Mechanisms, and Time-Varying Codes, *International Journal of Computer Mathematics*, vol. 79(10), 1083-1091, 2002.
25. F.L. Țiplea, E. Mäkinen: A Note on SE-systems and Regular Canonical Systems, *Fundamenta Informaticae*, vol. 46(3), 253-256, 2001.
26. F.L. Țiplea, E. Mäkinen: A Note on Synchronized Extension Systems, *Information Processing Letters*, vol. 79, 7-9, 2001.
27. F.L. Țiplea, E. Mäkinen, C. Apachițe: Syncronized Extension Systems, *Acta Informatica*, vol. 37, 449-465, 2001.
28. F.L. Țiplea, C. Ene, C.M. Ionescu, O. Procopiuc: Some Decision Problems for Parallel Communicating Grammar Systems, *Theoretical Computer Science*, vol. 134, 365-385, 1994.
29. C.M. Ionescu, O. Procopiuc, F.L. Țiplea: Parallel Communicating Grammar Systems: the Context-Sensitive Case, *International Journal of Computer Mathematics*, vol. 49(3-4), 145-156, 1993, https://doi.org/10.1080/00207169308804225.
30. F.L. Țiplea: Selective Petri Net Languages, *International Journal of Computer Mathematics*, vol. 43(1+2), 61-80, 1992.

Papers in Web of Science indexed journals and conferences (without impact factor)

All papers in this section are visible in Web of Science, ResearcherID B-9674-2011

1. F.L. Țtiplea, C. Hristea, D. Gîfu: Efficient RFID Scheme in Healthcare Systems. *KES 2023*: 3996-4005.
2. F.L. Țiplea: A Brief Introduction to Quadratic Residuosity Based Cryptography, *Revue Roumaine de Mathematiques Pures et Appliquees*, vol. 66, issue 3-4, 793-811, 2021, http://imar.ro/journals/Revue_Mathematique/pdfs/2021/3-4/18.pdf.

3. F.L. Țiplea, C. Hristea: Practically Efficient RFID Scheme with Constant-time Identification, Proceedings of the *18th International Conference on Security and Cryptography*, SECRYPT 2021, 495-506, July 6-8, 2021.
4. F.L. Țiplea, A. Ionita, A.-M. Nica: Practically Efficient Attribute-based Encryption for Compartmented Access Structures, in Proceedings of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020) - SECRYPT: 201-212.
5. A.-M. Nica, F.L. Țiplea: On Anonymization of Cocks' Identity-based Encryption Scheme, *Comput. Sci. J. Moldova*, vol. 27(3), 283-298, 2019.
6. F.L. Țiplea, C. Vârlan: Group Anonymity in Security Protocols, *FedCSIS – C&SS 2018*: 407-416.
7. F.L. Țiplea, C. Drăgan, A.-M. Nica: Key-Policy Attribute-Based Encryption from Bilinear Maps, *10th International Conference SECITC 2017*, LNCS 10543, 28-42, 2017.
8. F.L. Țiplea, S. Iftene, G. Teșeleanu, A.-M. Nica: Security of Identity-based Encryption Schemes from Quadratic Residuosity, *9th International Conference SECITC*, 9-10 June 2016, LNCS 10006, 63-74.
9. G.D. Năstase, F.L. Țiplea: 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).
10. F.L. Țiplea, C. Drăgan: 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).
11. F.L. Țiplea, L. Vamanu, C. Vârlan: 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.
12. L. Cojocaru, E. Makinen and F. L. Țiplea: 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.
13. F.L. Țiplea, 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.
14. I. Leahu, F.L. Țiplea: 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.
15. F.L. Țiplea, A. Țiplea: 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.

16. F.L. Țiplea, 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.
17. F.L. Țiplea, A. Țiplea: A Compositional Semantics for Petri Net Reactive Modules, *NATO Advanced Research Workshop CIPC2003*, Sinaia (Romania), IOS Press, vol. 195, 131-145, 2005.

Papers in other International Databases indexed journals

Most papers in this section are visible in DBLP https://dblp.org/pid/16/4077.html.

1. F.L. Țiplea, 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.
2. R. Melinte, O. Oanea, I. Olga, F.L. Țiplea: The Home Marking Problem and Some Related Concepts, *Acta Cybernetica*, vol. 15(3), 467–478, 2002.
3. F.L. Țiplea, E. Mäkinen: On the Complexity of a Problem on Monadic String Rewriting Systems, *Journal of Automata, Languages and Combinatorics* 7(4), 599-609, 2002.
4. F.L. Țiplea, C. Badarau: A Note on Decidability of Reachability for Conditional Petri Nets, *Acta Cybernetica* 14, 455-459, 2000.
5. F.L. Țiplea, A. Țiplea: On Normalization of Petri Nets, *Scientific Annals of the ``Al.I.Cuza'' University of Iasi*, Computer Science Section, Tome VIII, 151-161, 1999.
6. F.L. Țiplea, E. Mäkinen: Jumping Petri Nets. Specific Properties, *Fundamenta Informaticae*, vol. 32, 373-392, 1997.
7. F.L. Țiplea, M. Katsura, M. Ito: Processes and Vectorial Characterizations of Parallel Communicating Grammar Systems, *Journal of Automata, Languages and Combinatorics* 2, 47-73, 1997.
8. E. Mäkinen, F.L. Țiplea: Pattern Preserving Ambiguities for Pure Context-Free Grammars, *Fundamenta Informaticae*, vol. 30, 183-191, 1997.
9. F.L. Țiplea, C. Ene: Hierarchies of Petri Net Languages and a Super-Normal Form, *Journal of Automata, Languages and Combinatorics* 2, 187-204, 1997.
10. F.L. Țiplea, M. Katsura, M. Ito: On a Normal Form of Petri Nets, *Acta Cybernetica* 12, 295-308, 1996.
11. F.L. Țiplea, T. Jucan: Jumping Petri Nets, Foundations of Computing and Decision Sciences 19, no. 4, 319-332, 1994, http://fcds.cs.put.poznan.pl/FCDS/Old/1994.htm.
12. F.L. Țiplea, C. Ene: A Coverability Structure for Parallel Communicating Grammar Systems, *Journal of Information Processing and Cybernetics* EIK 29, no. 5, 303-315, 1993.

13. F.L. Țiplea, T. Jucan, C. Masalagiu: Relation Based Controlled Petri Nets, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Inf. 1, 27-35, 1993.
14. F.L. Țiplea: On Place Restricted Petri Nets, *Foundation of Computing and Decision Sciences* 16, no.1, 29-38, 1991, http://fcds.cs.put.poznan.pl/FCDS/Old/1991.htm.
15. F.L. Țiplea, T. Jucan, C. Masalagiu: Conditional Petri Net Languages, *Journal of Information Processing and Cybernetics* EIK 27, no.1, 55-66, 1991.
16. F.L. Țiplea: Reversible and Strict Reversible P/T-Systems, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Math.-Inf. 34, no.4, 319-327, 1988.
17. F.L. Țiplea, T. Jucan, C. Masalagiu: Term Rewriting Systems and P/T-Nets, Scientific *Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Math.-Inf. 34, no.4, 305-317, 1988.
18. T. Jucan, C. Masalagiu, F.L. Țiplea: Sufficient Conditions for the Decidability of s->*t, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Math. -Inf. 34, no. 4, 295-303, 1988.

Papers in other international conferences, symposiums, workshops

1. F.L. Țiplea, V.-F. Drăgoi: Generalized Inverse Based Decoding, The *2022 IEEE International Symposium on Information Theory (ISIT)*, June 26-July 1, 2022, Aalto University in Espoo, Finland.
2. F. Belardinelli, C. Dima, V. Malvone, F.L. Țiplea: A Hennessy-Milner Theorem for ATL with Imperfect Information, LICS 2020: 181-194.
3. C. Hristea, F.L. Țiplea: A PUF-Based Destructive Private Mutual Authentication RFID Protocol, SecITC 2018: 331-343.
4. C. Dragan, F.L. Țiplea: 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).
5. F.L. Țiplea, E. Simion: New Results on IBE from Quadratic Residuosity, 8th International Conference SECITC 2015, Bucharest, Romania, June 11-12, LNCS 9522, pag xiv-xvi, 2015.
6. F.L. Țiplea: 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).
7. F. Hamza-Lup, F.L. Țiplea: 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.

8. F.L. Țiplea, 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*, Țimisoara (Romania), March 17-22, 2005, IOS Press 2006, 185-211.
9. F.L. Țiplea, 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.
10. F.L. Țiplea, 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.
11. R. Melinte, O. Oanea, I. Olga, F.L. Țiplea: The Home Marking Problem and Some Related Concepts, PROMISE 2002, Potsdam (Germany), 2002, Lecture Notes in Informatics, 104-115.
12. F.L. Țiplea, A. Țiplea: 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.
13. F.L. Țiplea, E. Mäkinen: Jumping Petri Nets. Specific Properties, Proc. of the the 3rd International Conference ``Developments in Language Theory", Thessaloniki (Greece), pag 461-476, 1997.
14. C. Matei, F.L. Țiplea: (0,1)-Total Pure Context-Free Grammars, Proc. of the 2nd International Conference "Developments in Language Theory", Magdeburg, Germany, 1995, 148-153.
15. F.L. Țiplea, 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.
16. F.L. Țiplea, 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.

Other papers and presentations

1. F.L. Țiplea: The way to modern cryptography, Workshop on Circuits, Systems and Information Technology, WCSIT 2014.
2. F.L. Țiplea: Identity-based Encryption, Romanian Cryptology Days, 2013.
3. F.L. Țiplea: Modeling and Analysis of Security Protocols, Romanian Cryptology Days, 2011.
4. C. Dima, C. Enea, D. Guelev, F.L. Țiplea: 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.

5. F.L. Țiplea, C. Birjoveanu, C. Enea: Complexity of the Secrecy Problem for Bounded Security Protocols, NATO Advanced Research Workshop on Information Security for Wireless Networks, Suceava (Romania), Sept 4-8, 2006.
6. F.L. Țiplea, J. Desel: Petri Net Process Decomposition with Application to Validation, Proc. of the 6th Conference on Algorithms and Tools for Petri Nets, Frankfurt am Main (Germany), Oct 11-12, 61-68, 1999.
7. F.L. Țiplea, A. Țiplea: On Normalization of Petri Nets, Proc. of the 11th Romanian Symposium on Computer Science ROSYCS'98, Iasi (Romania), May 1998.
8. F.L. Țiplea, T. Jucan: Complexity of Petri Nets, Proc. of the 10th Romanian Symposium on Computer Science ROSYCS'96, Iasi (Romania), May 1996, 1-26.
9. F.L. Țiplea, T. Jucan: Petri Net Languages, Proc. of the 10th Romanian Symposium on Computer Science ROSYCS'96, Iasi (Romania), May 1996, 71-96.
10. F.L. Țiplea: 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.
11. F.L. Țiplea, 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.
12. F.L. Țiplea: Petri Net Languages, Proc. of the 19th Symposium on Semigroups, Languages and their Related Fields, Shimane (Japan), 1995, 71-86.
13. F.L. Țiplea, G. Macovei: Selective Grammars, *Annals of the University of Bucharest*, Ser. Math. -Inform. 61-68, 1995.
14. F.L. Țiplea: 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.
15. C. Masalagiu, T. Jucan, F.L. Țiplea: 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.
16. F.L. Țiplea, 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.
17. C. Masalagiu, T. Jucan, F.L. Țiplea: A Refinement of the Matching Extension Operations, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Math.-Inf. 35, no.4, 343-351, 1989.
18. F.L. Țiplea, T. Jucan, C. Masalagiu: Matching Extensions for Petri Net Languages, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Math.-Inf. 35, no.4, 337-342, 1989.
19. F.L. Țiplea, 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.
20. F.L. Țiplea: On General Unification, *Mathematical Reports* 40, no. 2, 161-172, 1988.

21. F.L. Țiplea: Almost Regular ACFM Theories, Proc. of the 6th Symposium on Computer Science INFO-IASI, Iasi (Romania), Oct 9 - 10, 1987, 192-201.

May 28, 2024 Prof.dr. Ferucio Laurențiu ȚIPLEA