Ferucio Laurențiu Țiplea

Publications

Books:

1. F.L. Tiplea: Algebraic Foundations of Computer Science. First edition: Polirom, 2006 (581+xiii pages). Second edition: "Alexandru Ioan Cuza" University Publishing House, ISBN 978-606-714-630-1, April 2021 (605 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, "Alexandru Ioan Cuza" University Publishing House, Iasi, 1998 (306 + xiv pages)

4. T. Jucan, F.L. Tiplea: Petri Nets, "Alexandru Ioan 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. 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 Published in Refereed Journals:

1. F.L. Tiplea, C. Hristea: PUF Protected Variables: A Solution to RFID Security and Privacy Under Corruption with Temporary State Disclosure, *IEEE Trans. Inf. Forensics Secur.*, vol 16, 999-1013, 2021

2. F.L Tiplea, S. Iftene, G. Teseleanu, A.-M. Nica: On the Distribution of Quadratic Residues and Non-residues Modulo Composite Integers and Applications to Cryptography, *Appl. Math. Comput.* 372, 2020

3. C. Hristea, F.L. Tiplea: Privacy of Stateful RFID Systems With Constant Tag Identifiers, *IEEE Trans. Inf. Forensics Secur.* 15: 1920-1934, 2020

4. A.-M. Nica, F.L. Tiplea: On Anonymization of Cocks' Identity-based Encryption Scheme, *Comput. Sci. J. Moldova* 27(3): 283-298, 2019

5. C. Dragan, F.L. Tiplea: On the Asymptotic Idealness of the Asmuth-Bloom Threshold Secret Sharing Scheme, *Information Sciences*, vol. 463–464, Oct 2018, 75-85.

6. C. Dragan, F.L. Tiplea: Distributive Weighted Threshold Secret Sharing Schemes, *Information Sciences*, 339, 85-97, January 2016

7. 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

8. 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

9. F.L. Tiplea, R. Diaconu: Petri Net Computers and Workflow Nets, *IEEE Transactions on SMC: Systems*, 45(3), 498-507, August 2014

10. 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

11. 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

12. F.L. Tiplea, C. Bocaneala: Priority Workflow Nets, *IEEE Transactions on Systems, Man and Cybernetics: Systems*, vol. 43(2), 2013, 402-415

13. 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

14. F.L. Tiplea, L. Vamanu, C. Varlan: Reasoning about Minimal Anonymity in Security Protocols, *Future Generation Computer Systems* (Elsevier), 29(3), 2013, 828-842

15. 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

16. 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

17. 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

18. F.L. Tiplea, A. Tiplea: Petri Net Reactive Modules, *Theoretical Computer Science* 359, 2006, 77-100

19. F.L. Tiplea, C. Enea: Abstractions of Data Types, *Acta Informatica* 42(8-9), 2006, 639-671

20. F.L. Tiplea, D.C. Marinescu: Structural Soundness for Workflow Nets is Decidable, *Information Processing Letters* 96, 2005, 54-58

21. F.L. Tiplea, E. Mäkinen, D. Trinca, C. Enea: Characterization Results for Time-Varying Codes, *Fundamenta Informaticae* 52, 2002, 1-13

22. R. Melinte, O. Oanea, I. Olga, F.L. Tiplea: The Home Marking Problem and Some Related Concepts, *Acta Cybernetica* 15(3), 2002

23. 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

24. 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

25. F.L. Tiplea, E. Mäkinen: A Note on SE-systems and Regular Canonical Systems, *Fundamenta Informaticae* 46, 3 (2001), 253-256

26. F.L. Tiplea, E. Mäkinen: A Note on Synchronized Extension Systems, *Information Processing Letters* 79, 2001, 7-9

27. F.L. Tiplea, E. Mäkinen, C. Apachite: Syncronized Extension Systems, *Acta Informatica* 37, 2001, 449-465

28. F.L. Tiplea, C. Badarau: A Note on Decidability of Reachability for Conditional Petri Nets, *Acta Cybernetica* 14, 2000, 455-459

29. 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

30. F.L. Tiplea, E. Mäkinen: Jumping Petri Nets. Specific Properties, *Fundamenta Informaticae* 32, 1997, 373-392

31. E. Mäkinen, F.L. Tiplea: Pattern Preserving Ambiguities for Pure Context-Free Grammars, *Fundamenta Informaticae* 30, 1997, 183-191

32. 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

33. F.L. Tiplea, M. Katsura, M. Ito: On a Normal Form of Petri Nets, *Acta Cybernetica* 12, 1996, 295-308

34. F.L. Tiplea, G. Macovei: Selective Grammars, *Annals of the University of Bucharest*, Ser. Math. -Inform. 1995, 61-68

35. 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

36. 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

37. F.L. Tiplea, T. Jucan: Jumping Petri Nets, Foundations of Computing and Decision Sciences 19, no. 4, 1994, 319-332

38. 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

39. 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

40. F.L. Tiplea, T. Jucan, C. Masalagiu: Relation Based Controlled Petri Nets, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Inf. 1, 1993

41. F.L. Tiplea: Selective Petri Net Languages, *International Journal of Computer Mathematics* 43, no.1+2, 1992, 61-80

42. F.L. Tiplea: On Place Restricted Petri Nets, *Foundation of Computing and Decision Sciences* 16, no.1, 1991, 29-38

43. F.L. Tiplea, T. Jucan, C. Masalagiu: Conditional Petri Net Languages, *Journal of Information Processing and Cybernetics* EIK 27, no.1, 1991, 55-66

44. C. Masalagiu, T. Jucan, F.L. Tiplea: A Refinement of the Matching Extension Operations, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Math.-Inf. 35, no.4, 1989, 343-351

45. F.L. Tiplea, 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, 1989, 337-342

46. F.L. Tiplea: Reversible and Strict Reversible P/T-Systems, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Math.-Inf. 34, no.4, 1988, 319-327

47. F.L. Tiplea, 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, 1988, 305-317

48. T. Jucan, C. Masalagiu, F.L. Tiplea: Sufficient Conditions for the Decidability of s->*t, *Scientific Annals of the "Alexandru Ioan Cuza" University of Iasi*, Section Math.-Inf. 34, no. 4, 1988, 295-303

49. F.L. Tiplea: On General Unification, *Mathematical Reports* 40, no. 2, 1988, 161-172

Papers Presented at Refereed Conferences:

1. F.L. Tiplea, C. Hristea: Practically Efficient RFID Scheme with Constant-time Identification, SECRYPT 2021: 495-506

2. F.L. Tiplea, A. Ionita, A.-M. Nica: Practically Efficient Attribute-based Encryption for Compartmented Access Structures, ICETE (2) 2020: 201-212

3. F. Belardinelli, C. Dima, V. Malvone, F.L. Tiplea: A Hennessy-Milner Theorem for ATL with Imperfect Information, LICS 2020: 181-194

4. F.L. Tiplea, Cosmin Vârlan: Group Anonymity in Security Protocols, FedCSIS – C&SS 2018: 407-416

5. C. Hristea, F.L. Tiplea: A PUF-Based Destructive Private Mutual Authentication RFID Protocol, SecITC 2018: 331-343

6. 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

7. 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

8. 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)

9. F.L. Tiplea, E. Simion: New Results on IBE from Quadratic Residuosity, 8th International Conference SECITC 2015, Bucharest, Romania, June 11-12, 2015

10. 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)

11. 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)

12. 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)

13. F.L. Tiplea: The way to modern cryptography, Workshop on Circuits, Systems and Information Technology, WCSIT 2014

14. F.L. Tiplea: Identity-based Encryption, Romanian Cryptology Days, 2013

15. F.L. Tiplea: Modeling and Analysis of Security Protocols, Romanian Cryptology Days, 2011

16. 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

17. 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

18. 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

19. 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

20. 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

21. 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)

22. 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)

23. 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

24. 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

25. 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

26. 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

27. 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

28. 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)

29. 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

30. 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

31. 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

32. 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

33. 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

34. F.L. Tiplea, E. Mäkinen: Jumping Petri Nets. Specific Properties, Proc. of the the 3rd International Conference ``Developments in Language Theory'', Thessaloniki (Greece), 1997

35. 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

36. 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

37. 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

38. 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

39. F.L. Tiplea: Petri Net Languages, Proc. of the 19th Symposium on Semigroups, Languages and their Related Fields, Shimane (Japan), 1995, 71-86

40. 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

41. 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

42. F.L. Tiplea: Jumping Petri Nets, 7th International Conference on Automata and Formal Languages, Salgotarjan (Hungary), 1993

43. 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

44. 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

45. 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

46. 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

47. 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

48. 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

Oct 5, 2021

Prof.dr. Ferucio Laurentiu Tiplea