Luca Mariot

Curriculum Vitae

Education

Dec 2014 – Mar 2018 **PhD in Computer Science (Double Degree)**, *University of Milano-Bicocca (Italy) and University of Côte d'Azur (France)*, Graduated with honours.
Thesis: Cellular Automata, Boolean Functions and Combinatorial Designs
Supervisors: prof. Alberto Leporati and prof. Enrico Formenti

Nov 2010 – Sep 2013 **M.Sc. in Computer Science**, *University of Milano-Bicocca (Italy)*, Final Mark: 110/110 cum laude.
Thesis: Cryptographic Pseudorandom Number Generators Based on Chaotic Cellular Automata
Supervisors: prof. Alberto Leporati and prof. Alberto Dennunzio

Oct 2006 – Nov 2010 **B.Sc. in Computer Science**, *University of Milano-Bicocca (Italy)*, Final Mark: 100/110.
Thesis: Cryptographic Hash Functions Based on Cellular Automata
Supervisors: prof. Alberto Leporati and prof. Claudio Ferretti

Experience

Jan 2018 – Present **Postdoctoral Research Fellow**, *University of Milano-Bicocca (Italy)*.
Research project: Natural Computing Models and Techniques for Cryptography

Feb 2014 – Nov 2014 **Graduate Research Scholarship**, *Consorzio Milano Ricerche and University of Milano-Bicocca (Italy)*.
Research project: Study and design of anonymization algorithms to enforce privacy in the management of prescription data

Mar 2013 – Sep 2013 **Research Internship**, *University of Milano-Bicocca (Italy*.
Research project: Analysis of the cryptographic properties of cellular automata for designing pseudorandom number generators

Publications

Journal Papers

[j4] L. Mariot, S. Picek, A. Leporati, D. Jakobovic. Cellular automata based S-boxes. Cryptography and Communications (in press). DOI: 10.1007/s12095-018-0311-8

[j3] L. Mariot and A. Leporati. A cryptographic and coding-theoretic perspective on the global rules of cellular automata. Natural Computing 17(3): 487-498 (2018)

[j2] L. Mariot, A. Leporati, A. Dennunzio, and E. Formenti. Computing the periods of preimages in surjective cellular automata. Natural Computing, 16(3):367–381 (2017)

[j1] A. Leporati and L. Mariot. Cryptographic properties of bipermutive cellular automata rules. J. Cellular Automata, 9(5-6):437–475 (2014)

Department of Informatics, Systems and Communications
University of Milano-Bicocca, Italy
+39 02 6448 7858 • *luca.mariot@disco.unimib.it*
lucamariot.org

Conference Papers

[c17] J. García-Duro, L. Manzoni, I. Arias, M. Casal, O. Cruz, X. M. Pesqueira, A. Muñoz, R. Álvarez, L. Mariot, S. Bandini, O. Reyes: Hidden Costs of Modelling Post-fire Plant Community Assembly Using Cellular Automata. In: Proceedings of ACRI 2018. pp. 68-79 (2018)

[c16] L. Mariot, A. Leporati: Inversion of Mutually Orthogonal Cellular Automata. In: Proceedings of ACRI 2018. pp. 364-376 (2018)

[c15] L. Manzoni, L. Mariot: Cellular Automata Pseudo-Random Number Generators and Their Resistance to Asynchrony. In: Proceedings of ACRI 2018. pp. 428-437 (2018)

[c14] S. Picek, K. Knezevic, L. Mariot, D. Jakobovic, A. Leporati: Evolving Bent Quaternary Functions. In: Proceedings of CEC 2018. pp. 1-8 (2018)

[c13] L. Mariot, S. Picek, D. Jakobovic, A. Leporati: Evolutionary Search of Binary Orthogonal Arrays. In: Proceedings of PPSN (1) 2018. pp. 121-133 (2018)

[c12] K. Knezevic, S. Picek, L. Mariot, A. Leporati, D. Jakobovic. The Design of (Almost) Disjunct Matrices by Evolutionary Algorithms. In: Proceedings of TPNC 2018 (in press). DOI: 10.1007/978-3-030-04070-3_12

[c11] L. Mariot, E. Formenti, A. Leporati: Enumerating Orthogonal Latin Squares Generated by Bipermutive Cellular Automata. In: Proceedings of AUTOMATA 2017. pp. 151-164 (2017)

[c10] S. Picek, L. Mariot, B. Yang, D. Jakobovic, N. Mentens: Design of S-boxes Defined with Cellular Automata Rules. In: Proceedinfs of Conf. Computing Frontiers 2017. pp. 409-414 (2017)

[c9] S. Picek, L. Mariot, A. Leporati, D. Jakobovic: Evolving S-boxes based on cellular automata with genetic programming. In: Proceedings of GECCO (Companion) 2017. pp. 251-252 (2017)

[c8] L. Mariot, S. Picek, D. Jakobovic, A. Leporati: Evolutionary algorithms for the design of orthogonal latin squares based on cellular automata. In: Proceedings of GECCO 2017. pp. 306-313 (2017)

[c7] L. Mariot, A. Leporati: Resilient Vectorial Functions and Cyclic Codes Arising from Cellular Automata. In: Proceedings of ACRI 2016. pp. 34-44 (2016)

[c6] L. Mariot: Asynchrony Immune Cellular Automata. In: Proceedings of ACRI 2016. pp. 176-181 (2016)

[c5] L. Mariot, A. Leporati: On the Periods of Spatially Periodic Preimages in Linear Bipermutive Cellular Automata. In: Proceedings of AUTOMATA 2015. pp. 181-195 (2015)

[c4] L. Mariot, A. Leporati: Heuristic Search by Particle Swarm Optimization of Boolean Functions for Cryptographic Applications. In: Proceedings of GECCO (Companion) 2015. pp. 1425-1426 (2015)

[c3] L. Mariot, A. Leporati: A Genetic Algorithm for Evolving Plateaued Cryptographic Boolean Functions. In: Proceedings of TPNC 2015. pp. 33-45 (2015)

[c2] L. Mariot, A. Leporati: Sharing Secrets by Computing Preimages of Bipermutive Cellular Automata. In: Proceedings of ACRI 2014. pp. 417-426 (2014)

[c1] Alberto Leporati, Luca Mariot: 1-Resiliency of Bipermutive Cellular Automata Rules. In: Proceedings of AUTOMATA 2013. pp. 110-123 (2013)

Visiting Periods

Apr 2016 – Mar 2017 *Visiting PhD student at Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis (I3S), Université Côte d'Azur (France)*

Participation in Committees

Program Committees

- 13th International Conference Cellular Automata for Research and Industry (ACRI 2018)

Organizing Committees

- 13th International Conference Cellular Automata for Research and Industry (ACRI 2018)
- 23rd International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA 2017)

Reviewing Activity

- Natural Computing
- Journal of Optimization
- Applied Soft Computing
- Journal of Cellular Automata
- The World Scientific Journal

Teaching Activity

Mar 2018 – Jun 2018 Teaching Assistant for *Theoretical Computer Science*, Department of Information Engineering, University of Bergamo (16 hours)

Mar 2018 – Jun 2018 Teaching Assistant for *Information Theory and Cryptography*, Department of Informatics, Systems and Communications, University of Milano-Bicocca (10 hours)

Mar 2018 – Jun 2018 Teaching Assistant for *Laboratory of Computer Science*, Department of Physics, University of Milano-Bicocca (20 hours)

Mar 2018 – Jun 2018 Teaching Assistant for *Algorithms and Computer Programming*, Department of Mathematics, University of Milano-Bicocca (12 hours)

Oct 2017 – Jan 2018 Teaching Assistant for *Languages and Computability*, Department of Informatics, Systems and Communications, University of Milano-Bicocca (12 hours)

Mar 2017 – Jun 2017 Teaching Assistant for *Information Theory and Cryptography*, Department of Informatics, Systems and Communications, University of Milano-Bicocca (10 hours)

Oct 2015 – Jan 2016 Teaching Assistant for *Programming Languages*, Department of Informatics, Systems and Communications, University of Milano-Bicocca (10 hours)

Oct 2015 – Jan 2016 Teaching Assistant for *Computer Programming*, Department of Informatics, Systems and Communications, University of Milano-Bicocca (24 hours)

Department of Informatics, Systems and Communications
University of Milano-Bicocca, Italy
+39 02 6448 7858 • *luca.mariot@disco.unimib.it*
lucamariot.org