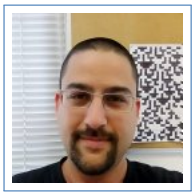

Luca Mariot

Curriculum Vitae

Experience

Jan 2018 – Present **Postdoctoral Researcher**, *University of Milano-Bicocca (Italy)*.
Research project: Natural computing models and techniques for cryptography

Dec 2014 – Dec 2018 **PhD Researcher**, *University of Milano-Bicocca (Italy)*.
Research project: Cryptographic applications of cellular automata and their relations to Boolean functions and combinatorial designs

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

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 honors.
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

Publications

Journal Papers

[j4] L. Mariot, S. Picek, A. Leporati, D. Jakobovic: *Cellular automata based S-boxes*. Cryptography and Communications 11(1): 41-62 (2019)

[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)

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

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

Conference Papers

[c19] L. Manzoni, L. Mariot, E. Tuba: *Does constraining the search space of GA always help?: the case of balanced crossover operators*. In: Proceedings of GECCO (Companion) 2019. pp. 151-152 (2019)

[c18] L. Mariot, D. Jakobovic, A. Leporati, S. Picek: *Hyper-bent Boolean Functions and Evolutionary Algorithms*. In: Proceedings of EUROGP 2019. pp. 262-277 (2019)

[c19] C. Ferretti, A. Leporati, L. Mariot, L. Nizzardo: *Transferable Anonymous Payments via TumbleBit in Permissioned Blockchains*. In: Proceedings of DLT@ITASEC 2019. pp. 56-67 (2019)

[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. pp. 152-163 (2018)

[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: Proceedings 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)

Talks

Invited Seminar Talks

18 Mar 2019 *Cryptographic Criteria of Boolean Functions and S-Boxes.* Guest Lecture for Digital Communication course, Durham University, UK

19 Jun 2018 *Open problems in the design of cryptographic applications based on Cellular Automata.* Cyber Security Seminar at TU Delft, The Netherlands

30 Jan 2018 *Cryptographie avec les Automates Cellulaires* (in French). MC3 Seminar at I3S Laboratory, University of Nice Sophia Antipolis, France

14 Nov 2017 *Cryptography by Cellular Automata.* Seminar for IEEE Croatia Section – Computational Intelligence Chapter, University of Zagreb, Croatia

12 Apr 2016 *Cyclic Codes and Cellular Automata.* Seminar at Journées Calculabilités 2016, University of Nice Sophia Antipolis, France

16 Apr 2014 *Cryptographic Properties and Applications of Bipermutive Cellular Automata.* MC3 Seminar at I3S Laboratory, University of Nice Sophia Antipolis, France

Contributed Talks in Conferences

20 Sep 2018 *Inversion of Mutually Orthogonal CA.* ACRI 2018, Como, Italy

18 Sep 2018 *Cellular Automata Pseudo-Random Number Generators and Their Resistance to Asynchrony* (joint talk with Luca Manzoni). ACRI 2018, Como, Italy

18 Jul 2017 *Evolutionary Algorithms for the Design of Orthogonal Latin Squares based on CA.* GECCO 2017, Berlin, Germany

8 Jun 2017 *Enumerating Orthogonal Latin Squares Generated by Bipermutive CA.* AUTOMATA 2017, Milan, Italy

15 May 2017 *Design of S-boxes Defined with CA Rules.* CF 2017, Siena, Italy

7 Sep 2016 *Asynchrony Immune CA.* ACRI 2016, Fez, Morocco

5 Sep 2016 *Resilient Functions and Cyclic Codes from CA.* ACRI 2016, Fez, Morocco

15 Jun 2016 *Constructing Orthogonal Latin Squares from Linear CA.* AUTOMATA 2016, Zurich, Switzerland

15 Dec 2015 *A Genetic Algorithm for Evolving Plateaued Cryptographic Boolean Functions.* TPNC 2015, Mieres, Spain

10 Jun 2015 *On the Periods of Spatially Periodic Preimages in Linear Bipermutive CA.* AUTOMATA 2015, Turku, Finland

25 Sep 2014 *Sharing Secrets by Computing Preimages of Bipermutive CA.* ACRI 2014, Krakow, Poland

17 Sep 2013 *1-Resiliency of Bipermutive CA Rules.* AUTOMATA 2013, Giessen, Germany

Visiting Periods

10–24 Mar 2019 *Visiting Researcher at Department of Computer Science, Durham University (UK)*

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

Grants

Travel grant awarded by COST action IC1405 for a Short-Term Scientific Mission at Durham University, UK, on March 10-24 2019 (amount awarded: 1900 €)

Travel grant awarded by COST Action IC1306 to attend the training school "Symmetric Cryptography and Blockchain" in Torremolinos, Spain, February 19-23, 2018 (amount awarded: 800 €)

Travel grant awarded by COST Action CA15140 to attend the training school "Improving Applicability of Nature-Inspired Optimisation by Joining Theory and Practice" in Paris, France, October 18-24, 2017 (amount awarded: 1420 €)

Travel grant awarded by ACM to attend the Genetic and Evolutionary Computation Conference 2017 in Berlin, Germany, July 15-17 2017 (amount awarded: 200 $)

Travel grant awarded by ACM to attend the Computing Frontiers Conference 2017 in Siena, Italy, May 15-17 2017 (amount awarded: 250 $)

Travel grant awarded by COST Action IC1306 to attend the training school "Randomness in Cryptography" in Barcelona, Spain, November 14-18 2016 (amount awarded: 800 €)

Reviewing Activity/Participation in Committees

Journals

Natural Computing, Applied Soft Computing, Journal of High Performance Computing, Journal of Optimization, Journal of Cellular Automata, The World Scientific Journal

Conferences

CIBB 2019, SETA 2018, AUTOMATA 2017, ACA 2016

Program Committees

- 5th Workshop on Cellular Automata Algorithms and Architectures (CAAA 2019)

- 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)

Teaching Activity

Phd Courses

May 2019 – Jun 2019 *Laboratory of population-based optimisation methods*, Department of Informatics, Systems and Communications, University of Milano-Bicocca. Co-taught with Dr. Luca Manzoni and Dr. Marco S. Nobile (20 hours)

Teaching Assistance in Bachelor-Master degrees

Oct 2018 – Jan 2019 *Computer Programming*, Department of Informatics, Systems and Communications, University of Milano-Bicocca (24 hours)

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

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

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

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

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

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

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

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

Theses Supervision

Master Joint supervision (with Alberto Leporati) of 1 student in the Master degree of Mathematics, and 2 students in the Master degree of Computer Science, University of Milano-Bicocca

References

Professor Alberto Leporati (alberto.leporati@unimib.it)

University of Milano-Bicocca, Milan, Italy

Professor Enrico Formenti (enrico.formenti@unice.it)

University of Côte d'Azur, Nice, France