



Luca Mariot

Curriculum Vitae

Experience

- 1 Dec 2022 – **Assistant Professor**, *Semantics, Cybersecurity and Services Group, University of Twente (The Netherlands)*
present
Research areas: cryptography, cybersecurity, AI, natural computing
- 1 Jan 2022 – **Postdoctoral Researcher**, *Digital Security Group, Radboud University in Nijmegen (The Netherlands)*
30 Nov 2022
Research topics: symmetric cryptography, evolutionary computation, security of AI
- 1 Mar 2020 – **Postdoctoral Researcher**, *Cyber Security Group, Delft University of Technology (The Netherlands)*
31 Dec 2021
Research topics: cryptography, evolutionary computation, cellular automata
- 1 Jan 2018 – **Postdoctoral Researcher**, *University of Milano-Bicocca (Italy)*
29 Feb 2020
Research project: Natural computing models and techniques for cryptography
- 1 Dec 2014 – **PhD Researcher**, *University of Milano-Bicocca (Italy) and University of Côte d'Azur (France)*
1 Dec 2017
Research project: Cryptographic applications of cellular automata
- 1 Feb 2014 – **Graduate Researcher**, *Consorzio Milano Ricerche (Italy)*
30 Nov 2014
Research project: anonymization algorithms for prescription data

Education

- 1 Dec 2014 – **PhD in Computer Science (Double Degree)**, *University of Milano-Bicocca (Italy) and University of Côte d'Azur (France)*, graduated with honors
9 Mar 2018
Thesis: Cellular Automata, Boolean Functions and Combinatorial Designs
Supervisors: prof. Alberto Leporati and prof. Enrico Formenti
- 1 Nov 2010 – **M.Sc. in Computer Science**, *University of Milano-Bicocca (Italy)*, Final Mark: 110/110 cum laude
26 Sep 2013
Thesis: Cryptographic Pseudorandom Number Generators Based on Chaotic Cellular Automata
Supervisors: prof. Alberto Leporati and prof. Alberto Dennunzio
- 1 Oct 2006 – **B.Sc. in Computer Science**, *University of Milano-Bicocca (Italy)*, Final Mark: 100/110
25 Nov 2010
Thesis: Cryptographic Hash Functions Based on Cellular Automata
Supervisors: prof. Alberto Leporati and prof. Claudio Ferretti

Publications

17 journal papers, **36** conference proceedings papers and **1** book chapter published in various peer-reviewed venues related to natural computing and cryptography.

2 conference papers selected as candidates for the best paper award ([c13] at PPSN 2018 and [c23] at EuroGP 2020), 1 paper selected as a finalist at the GECCO 2020 Humies competition ([c23]).

Google Scholar profile: <https://scholar.google.com/citations?user=I8Vq5WQAAAAJ&hl=en>

Visiting Periods

- 12 Sep – 31st Oct 2021 *Department of Informatics, Systems and Communications, University of Milano-Bicocca (Italy)*
- 13–20 Oct 2019 *Cyber Security Group, Intelligent Systems Department, Delft University of Technology (the Netherlands)*
- 22–29 Sep 2019 *Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis (I3S), Université Côte d'Azur (France)*
- 10–24 Mar 2019 *Department of Computer Science, Durham University (UK)*

Grants

2 travel grants awarded by MDPI Publishing to attend GECCO 2023

6 travel grants awarded by COST Actions CA15140, IC1405 and IC1306 to fund 2 Short-Term Scientific Missions at TU Delft and Durham University, and to attend 4 training schools on evolutionary computing and cryptography

2 travel grants awarded by ACM to attend GECCO 2017 and CF 2017

Selected Invited Talks

- 11 May 2023 *Adversarial Examples in Deep Learning and How to Fight Them.* Talk given at Beiersdorf, Hamburg, Germany
- 2 Nov 2022 *Behind the scenes of a new construction for bent functions.* Math Cifris Seminar, University of Trento, Italy
- 16 Oct 2021 *AI methods for the design of cryptographic primitives.* Workshop on Artificial Intelligence and Cryptography – AICrypt@EUROCRYPT 2021, Zagreb, Croatia

Service to the Academic Community

Reviewer for Journals

Designs, Codes and Cryptography; IEEE Transactions on Information Forensics & Security; Journal of Cryptographic Engineering; ACM Journal on Emerging Technologies in Computing Systems; Natural Computing; MDPI Algorithms; Applied Soft Computing; CIT Journal of Computing and Information Technologies; Journal of High Performance Computing; Journal of Optimization

Editor for Journals

- Jan 2023 - present Associate editor of the EURASIP Journal on Information Security (Q2 Scimago)
- Nov 2022 - present Guest editor of the special issue "Applications of Artificial Intelligence to Cryptography" for the journal MDPI Mathematics (Q2 Scimago)
- Oct 2021 - present Guest editor of the special issue "Algorithms for Natural Computing Models" for the journal MDPI Algorithms (Q2 Scimago)

Participation in Program Committees

NDSS 2024, AIHWS 2020-2023, APDCM 2022-2023, EvoAPPS 2023, ACRI 2018-2022, AUTOMATA 2022, IEEE CIBCB 2022 (special session), SPACE 2020-2022, WEPO 2020, CAAA 2019

Participation in Organizing Committees

IEEE CSF 2024 (general chair)
AUTOMATA 2023 (general and program chair)
IEEE Euro S&P 2023 (poster session chair)
CANS 2023 (publicity chair)
AICrypt@Eurocrypt 2023 (chair)
WEPO 2021 (chair)
ACRI 2018 (local organizer)
AUTOMATA 2017 (web chair, local organizer)

Participation in Steering Committees

IEEE CSF (mandate 2022-2027)

External Reviewer for Conferences/Workshops

CEC 2022, ACNS 2022, ASIACRYPT 2021, ESORICS 2021, NDSS 2020, DATE 2020, CIBB 2019, SETA 2018, AUTOMATA 2017, ACA 2016

Other Administrative Positions

Secretary of the IFIP Working Group 1.5 "Cellular Automata and Discrete Complex Systems" (mandate 2022-2024)

Professional Memberships

Member of IACR, EATCS, ACM SIGEVO, IEEE, IFIP WG 1.5

Teaching Activities

Teaching Training/Certifications

- Mar 2023 - present Currently undertaking the UTQ trajectory at the University of Twente (attended modules: course evaluation and course design)
- 13 Dec 2021 UTQ Certification – DEVELOP Module, Delft University of Technology, The Netherlands. Topics: Course design based on constructive alignment principles (40 hours)
- 31 Jan 2020 Qualification aux fonctions de maître de conférences, section 27, n. 20227333407

Teaching in PhD Courses

- June 25-30 2023 *AI and Cryptography*, PhD Program in Applied Data Science and Artificial Intelligence, University of Trieste (16 hours)
- May 2019 – *Laboratory of population-based optimisation methods*, PhD Program in Computer Science, University of Milano-Bicocca. Co-taught with Luca Manzoni and Marco S. Nobile (6 hours)

Guest Lectures

- 29 Mar 2023 *Public key cryptography, Diffie Hellmann key Exchange and RSA*. Guest lecture for Algebra & Cryptography CSE3230, TU Delft, The Netherlands
- 18 Mar 2019 *Cryptographic Criteria of Boolean Functions and S-Boxes*. Guest lecture for the Digital Communication course, Durham University, UK

Teaching Assistance in Bachelor-Master degrees

- Sep 2022 – *Introduction to Cryptography*, BSc in Computer Science, Radboud University (preparation of teaching materials, backup lecturer, grading exams)
- Feb 2022 – *Algebra & Cryptography*, BSc in Computer Science and Engineering, Delft University of Technology (12 hours, co-teaching the Algebra lectures)
- Mar 2022
- Jan 2021 – *Algebra & Cryptography*, BSc in Computer Science and Engineering, Delft University of Technology (32 hours, preparation of lecture materials, lead Q&A sessions)
- Apr 2021
- Mar 2020 *Algebra & Cryptography*, BSc in Computer Science and Engineering, Delft University of Technology (12 hours, preparation of teaching materials)
- Oct 2018 – *Computer Programming*, BSc in Computer Science, University of Milano-Bicocca
- Jan 2019 (24 hours, laboratory lectures)
- Mar 2018 – *Theoretical Computer Science*, MSc in Computer Engineering, University of Bergamo
- Jun 2018 (16 hours, exercises lectures)
- Mar 2018 – *Information Theory and Cryptography*, MSc in Computer Science, University of Milano-Bicocca (10 hours, exercises lectures)
- Jun 2018
- Mar 2018 – *Laboratory of Computer Science*, BSc in Physics, University of Milano-Bicocca (20 hours, laboratory lectures)
- Jun 2018
- Mar 2018 – *Algorithms and Computer Programming*, BSc in Mathematics, University of Milano-Bicocca (12 hours, laboratory lectures)
- Jun 2018
- Oct 2017 – *Languages and Computability*, BSc in Computer Science, University of Milano-Bicocca (12 hours, laboratory lectures)
- Jan 2018
- Mar 2017 – *Information Theory and Cryptography*, MSc in Computer Science, University of Milano-Bicocca (10 hours, exercises lectures)
- Jun 2017
- Oct 2015 – *Programming Languages*, BSc in Computer Science, University of Milano-Bicocca (10 hours, laboratory lectures)
- Jan 2016
- Oct 2015 – *Computer Programming*, BSc in Computer Science, University of Milano-Bicocca (24 hours, laboratory lectures)
- Jan 2016

Theses Supervision

Currently supervised students 1 master student in the Cybersecurity track of the master degree in Computer Science co-supervised at the University of Twente

Past supervised students 4 master students in Cybersecurity co-supervised at the TU Delft; 2 master students in Computer Science, 1 master student in Mathematics and 1 bachelor student in Computer Science co-supervised at the University of Milano-Bicocca

References

Stjepan Picek, Radboud University, The Netherlands (stjepan.picek@ru.nl)

Carlos A. Coello Coello, Cinvestav-IPN, Mexico (ccoello@cs.cinvestav.mx)

Mauro Castelli, NOVA IMS, Portugal (mcastelli@novaims.unl.pt)

Luca Manzoni, University of Trieste, Italy (lmanzoni@units.it)

Alberto Leporati, University of Milano-Bicocca, Italy (alberto.leporati@unimib.it)

Enrico Formenti, Université Côte d'Azur, France (enrico.formenti@unice.fr)

Date: 5/7/2023