Lorenzo Rovida
name.surname@{outlook, unimib}.it

3rd year PhD Student in Cryptography
Research interests: Homomorphic encryption · Lattice-based cryptography

Short bio

I am a PhD student at the University of Milano-Bicocca, and my main research field is Fully Homomorphic Encryption. Before that, I graduated in Computer Science and I worked for one year in the industry. During the first part of my PhD I worked on privacy-preserving applications such as encrypted images and texts classification using FHE schemes.

For the second part, I switched towards constructions of FHE schemes from a lattice-based perspective. So I am interested in better understand what happens, in geometrical terms, when we instantiate and use a FHE scheme.

During my PhD, I had some visiting periods in other universities/research institutes. In Spring/Summer 2024 I was hosted by at the Institut de Mathématiques de Bordeaux, and in Spring 2025 I was hosted by at COSIC, KU Leuven.

Education

University of Milano-Bicocca, Department of Computer Science, Milan, Italy
PhD in Cryptography
Enrolled: October 2022
Thesis submission: October 2025
Thesis proposal: *Homomorphic encryption: new constructions and algorithms*
Supervisor: Prof. Alberto Leporati

University of Milano-Bicocca, Department of Computer Science, Milan, Italy
Master Degree in Computer Science
Final votation: 110/110 *cum laude*
Period: September 2019 → October 2021
Final thesis name: *Implementation of a clustering algorithms based on Homomorphic Encryption*

Visiting experiences

COSIC, ESAT, KU Leuven Leuven, Belgium
Visiting the Computer Security and Industrial Cryptography (COSIC) group
Hosted by: Frederik Vercauteren
Period: April 2025 → June 2025

Institut de Mathématiques de Bordeaux (IMB), INRIA, University of Bordeaux, France
Visiting the Cryptography, ANalysis and ARIthmetic (CANARI) group
Hosted by: Wessel van Woerden
Period: May 2024 → September 2024

Publications in Journals and Conferences proceedings

Authors in publications with (*) are alphabetically ordered, so equal contribution, following the `American Mathematical Society statement`*, otherwise the order reflects the order of contribution*

All the publications are freely accessible as open-access documents or in the ePrint IACR *archive*

2025

- (*) (**Preprint**) Alberto Leporati, **Lorenzo Rovida** and Wessel van Woerden. *Beyond LWE: a Lattice Framework for Homomorphic Encryption.*
- (**Preprint**) **Lorenzo Rovida**, Alberto Leporati and Simone Basile. *Lightweight Sorting in Approximate Homomorphic Encryption.*
- Alberto Leporati and **Lorenzo Rovida**. *An Evolutionary Approach to the Design of Spiking Neural P Circuits.* In Journal of Membrane Computing, Special Issue Devoted to CMC 2024.

2024

- Alberto Leporati and **Lorenzo Rovida**. *Looking for Stability in Proof-of-Stake based Consensus Mechanisms.* In Blockchain: Research and Applications, pp. 100222.
- **Lorenzo Rovida** and Alberto Leporati. *Transformer-based Language Models and Homomorphic Encryption: An Intersection with $BERT_{tiny}$.* In Proceedings of the 10th ACM International Workshop on Security and Privacy Analytics pp. 3–13.
- **Lorenzo Rovida** and Alberto Leporati. *Encrypted Image Classification with Low Memory Footprint using Fully Homomorphic Encryption.* In International Journal of Neural Systems, Vol. 34, No. 5, pp. 2450025 (Pre-print at ia.cr/2024/460).

2023

- **Lorenzo Rovida**. *Fast but Approximate Homomorphic k-means Based on Masking Technique.* In International Journal of Information Security, Vol. 22, pp. 1605—1619

2020

- Chiara Damiani, **Lorenzo Rovida**, Davide Maspero, Irene Sala, Luca Rosato, Marzia Di Filippo, Dario Pescini, Alex Graudenzi, Marco Antoniotti and Giancarlo Mauri. *MaREA4Galaxy: Metabolic REaction Enrichment Analysis and Visualization of RNA-seq data within Galaxy.* In Computational and Structural Biotechnology Journal, Vol. 18, pp. 993–999

Presentations at International Conferences and Workshops

- 2024, Jun 21 – ACM CODASPY 2024 – 10th ACM International Workshop on Security and Privacy Analytics (*IWSPA 2024*) – University of Porto, Portugal. Presentation of the paper *Transformer-based Language Models and Homomorphic Encryption: an intersection with $BERT_{tiny}$.*
- 2024, Jun 3-5 – CMC 2024 – 25th Conference on Membrane Computing – Université Côte d'Azur – École Nationale Supérieure d'Arts à la Villa Arson, Nice, France. Presentation of the paper *An Evolutionary Approach to the Design of Spiking Neural P Circuits.*
- 2024, May 26 – Eurocrypt 2024 – 4rd Workshop on Artificial Intelligence and Cryptography (*AICrypt 2024*) – ETH Zurich, Switzerland. Presentation of the paper *Encrypted Image Classification with Low Memory Footprint with Fully Homomorphic Encryption.*
- 2023, April 22 – Eurocrypt 2023 – 3rd Workshop on Artificial Intelligence and Cryptography (*AICrypt 2023*) – ENS Lyon, France. Presentation of the paper *Fast but Approximate k-means based on Masking Technique.*

Talks

- 2025, Jun 17 – COSIC Seminar, ESAT, KU Leuven, *Lightweight sorting in approximate Homomorphic Encryption.*

Attended schools

- 2024, March 11-15 – Spring School on Post-Quantum Cryptography organized by Quantum-Safe Internet (QSI) - Porto, Portugal.

Teaching experiences

Frontal exercises (24 hours per A.Y)

- *Development of Mobile Applications* – Bachelor degree in Computer Science (8 CFU) - A.Y. 24/25, 25/26

Laboratory teaching (20 hours per A.Y.)

- *Development of Mobile Applications* – Bachelor degree in Computer Science (8 CFU) - A.Y. 23/24, 24/25, 25/26
- *Theory of Computability and Languages* – Bachelor degree in Computer Science (8 CFU) - A.Y. 22/23, 23/24, 24/25, 25/26

Tutoring activities

- *Mathematical Analysis 1* – Bachelor degree in Computer Science (8 CFU) – A.Y. 19/20, 20/21, 21/22, 23/24;
- *Machine Learning* – Master degree in Computer Science (6 CFU) – A.Y. 21/22;
- *Java Programming 2* – Bachelor degree in Computer Science (8 CFU) – A.Y. 20/21;
- *Thesis writing* – Bachelor/master degree in Computer Science (optional course) – A.Y. 23/24, 24/25;

Other activities

- *Introduction to Artificial Intellgence* (15 hours per A.Y.) – Course organized as part of the orientation for high schools – Funded by Piano Nazionale di Ripresa e Resilienza (PNRR) – A.Y. 22/23, 23/24, 24/25.
- Lecturer in the *Cyberchallenge* activity, a national Capture-The-Flag (CTF) challenge – Introduction to Software Security (12 hours) – A.Y 22/23, 23/24, 24/25.
- Tutor for students with Specific Learning Disorders at University of Milan-Bicocca – A.Y 22/23, 23/24.

Thesis co-supervisions

- Bachelor of Computer Science (University of Milano-Bicocca):
  - *About the impact of quantum computers on classical cryptography* (A.Y. 24/25)
- Master of Computer Science (University of Milano-Bicocca):
  - *Exploring fully homomorphic encryption for private information retrieval* (A.Y. 24/25)

Other talks

- 2023, December 21 – *Computing on Encrypted Data: an introduction to Homomorphic Encryption* – Talk given as part of PhD Seminars organized by the University of Milan-Bicocca.

Professional activities

- from 2020, January to *Now* – Solo game designer and developer for VERSEZERO (versezero.it), a mobile videogame jRPG developed with Unity 3D for Android and iPhones. Presented with a stand at the Milan Gamesweek (25-27 November 2022), one of the largest videogames exhibition in Italy. Demo available for both Android and iOS.
- from 2022, January to *Now* – Solo web developer and designer for a violinist teacher (eleonoraumidon.it).
- from 2022, November to 2023, September – Employee for Alten Italia. Worked on several C++ projects as a developer.
- from 2017 to 2020 – Developer for *Sanity*, a mobile application developed with Flutter and a Firebase backend, with the aim to help the connection between physiotherapists and patients (available on request).

Other

- Driving license **B**
- Full professional proficiency in English
- Limited working proficiency in Spanish