LEONARDO ERRATI

apprentice cryptographer

"a good plan goes a long way"

leonardoerrati.lwe@gmail.com
www.leonardoerrati.com

My interests include scientific communication, reading, learning, organising events.
I always strive to create.

SOFT SKILLS

Organisation and planning.
Bridging teams of different backgrounds. Adaptability.

HARD SKILLS

Programming:
Java, R, Python, Magma, C, React, Angular, MatLab, R.

Layout tools:
LaTex, Office, Beamer, Canva.

LANGUAGES

Italian	mother tongue
English	C1
German	still learning

REFERENCES

Dr. Alessio Meneghetti
research collaborator
alessio.meneghetti@unitn.it

Mattia A. Prando
Argentea internship supervisor
mattia.prando@argentea.it

ACADEMIC EXPERIENCE

PhD Student — Feb. 2025 - now
Politecnico di Torino, Italy
Doctoral position in the CrypTo group. I aim at partnering with national institution on various research projects.

Research fellow — Dec. 2024 - Jan. 2025
Università di Trento, Italy
Pre-doctoral fellowship on post-quantum solutions for digital identity. Created a partnership with institutions, e.g. Bank of Italy.

Research grant holder — June 2024 - Dec. 2024
Università di Trento, Italy
Pre-doctoral scholarship on threshold signatures and theoretical applications in blockchain. Partnered with research institutions.

University tutor — Sep. 2021 - Jan. 2024
Università di Trento, Italy
Linear algebra tutoring for degrees in informatics & engineering.

INDUSTRIAL EXPERIENCE

Research & development intern — March 2023 - Sep. 2023
Argentea SRL, Italy
Restructured the proprietary architecture for PAX terminals.
Planned a non-disruptive update for always-on terminals.

EDUCATION

Università di Trento, Italy — March 2024
Laurea Magistrale (master's degree) in Cryptography
Student representative. Cryptography, algebra, IT & network security. Thesis: Browkin's p-adic Continued Fractions.

Università di Trento, Italy — Nov. 2021
Laurea Triennale (bachelor's degree) in Mathematics
Pure mathematics, physics, statistics, probability, programming.
Thesis: history and architecture of Lucas' primality test(s).

PROJECTS

Project MIRAGE (member, researcher) — 2024 - now
Creation of a novel threshold signature scheme.

Project Archimedes (member) — 2021 - 2023
Creation of board games for scientific communication. Partnered with University of Trento and many high schools. Won the *"Mathematics at Play"* prize of StudioGiochi, Venice, in 2023.

Project Prometheus (founder) — *2018 - 2021*
Student initiative to write free and improved didactic material.
Created the unofficial Beamer theme for our Department.

VOLUNTEERING

Journal of Mathematical Cryptography
Peer reviewer for Number Theory and Cryptography areas.

De Componendis Cifris
Python & web developer, video editor, webmaster, organiser.

Liceo "Enrico Medi"
Assistant archaeologist. Science fair presenter.

Churches of Roverbella and Mozzecane
Organised trips and events, held contacts with external suppliers.

CERTIFICATES

Cryptography:
Trends24: the French Magisterium
Y2Y: Blockchain & Smart Contracts
Trends23: Cryptographic Protocols
Techniques in Coding Theory
Trends22: Modern Cryptography

Others:
Neuroscience Masterclass

AWARDS AND HONORS

Cyprus Tech Odyssey 2024   2024
University of Nicosia & XRPL Commons
First place with a whistleblowing project, allowing companies to safely comply with EU directive 2019/1937.

"Mathematics at Play" Archimede Prize   2023
StudioGiochi, Venezia
Our game from Project Archimedes won in the "Matematica in Gioco" area for the Archimede Prize.

Catch The Mark   *2022*
University of Trento
Devised a watermark attack granting first place.

IACR Travel Grant(s)   -
International Association of Cryptology
Awarded in 2023 and 2024 for participation at EuroCrypt.

TALKS HELD

Institutional speaker for *DeCifris*   2024
Cryptography Days 2024 & Combinatorics24, Italy
Speaker in the institutional sessions during some conferences.

Cultural evening "Math Talks"   2023
Scuola Arcivescovile, Trento
Organiser, speaker with *"Hamming, the man who defeated errors"*.

Seminar "MFA: handle with care"   *2022*
University of Trento & Bruno Kessler Foundation
Internal seminar on Multifactor Authentication for FBK.

Seminar "Quadratic sieve"   *2021*
University of Trento, Italy
Theoretical and practical aspects of quadratic sieve.

Seminar "Kant and the Age of Enlightenment"   2016
Liceo "Enrico Medi", Italy
Opening talk with prof. Simonetta Fortuna: Enlightenment in art.