Lorenzo Magliocco

PhD in Cybersecurity · Italian Citizen · Born December 1998
lmalloc · {last} (dot) {first} (at) gmail (dot) com · lorenzomagliocco.com · lorenzo-magliocco

About

I am a PhD in Cybersecurity who has carried out research in theoretical cryptography, with a background centered around engineering and computer science. My scientific contributions focus mostly on the design of foundational cryptographic protocols and theoretical models within cutting-edge Secure Multi-Party Computation settings. More broadly, I enjoy reasoning about adversarial behaviour in distributed systems, as well as low-level programming and network infrastructures.

Experience

Jun'26 - Aug'26 **Research Intern**, *Symbolic Software*
Under the supervision of Dr. Nadim Kobeissi, I contributed to the Ethereum Foundation's formal verification efforts by working towards the design of soundcalc-lean, a porting of the soundcalc tool in Lean4.

Feb'24 - Jun'24 **Visiting Researcher**, *The University of Edinburgh*
Under the supervision of Prof. Michele Ciampi, I investigated the problem of providing the first formalization of robust combiners for Non-Interactive Zero-Knowledge. I also took part to the activities of the Blockchain Technology Lab led by Prof. Aggelos Kiayias.

Education

Nov'22 - Jan'26 **PhD in Cybersecurity**, *Sapienza University of Rome & LUISS Guido Carli*
Final grade: Excellent, summa cum laude; Doctor Europaeus
Dissertation: The Mirage of Honesty in Cryptography: Secure MPC with Untrusted Devices
Supervisor: Prof. Daniele Venturi
Research keywords: PAKE, Subversion Resilience, Universal Composability, NIZK, Robust Combiners.

Oct'20 – Oct'22 **MSc in Cybersecurity**, *Sapienza University of Rome*
Final grade: 110/110, summa cum laude
Thesis: Subversion-Resilient Password-Authenticated Key Exchange in the UC Framework
Advisors: Prof. Daniele Venturi, Prof. Riccardo Lazzeretti
Salient coursework: Distributed Systems, Network Security, Malware Analysis, Risk Management.

Oct'17 – Oct'20 **BSc in Engineering in Computer Science**, *Sapienza University of Rome*
Final grade: 110/110, summa cum laude
Thesis: Introduzione a SPDZ
Advisors: Prof. Riccardo Lazzeretti
Salient coursework: Operating Systems, Telecommunications, Software Design, Economics.

Honors and Awards

May'24 **Laureato Eccellente**, *Fondazione Roma Sapienza*
Awarded for outstanding academic performance (AY 2021/2022).

Apr'23 **Premio di laurea in memoria del prof. Camil Demetrescu**, *DIAG Sapienza*
Awarded to the best two MSc theses in Cybersecurity among graduating peers of the Department of Engineering in Computer Science (AY 2021/2022).

Oct'22 **MSc Honours Programme**, *Sapienza University of Rome*
Awarded for successfully completing extracurricular research activities.
Topic: Code Analysis meets Adversarial Behaviour - MP-SPDZ vs Constantine + TEEs.

Jul'17 **Mention in the Albo Nazionale delle Eccellenze**, *Ministero dell'Istruzione e del Merito*
Awarded for outstanding performance in the national high-school final exams.

Academic Service

External Reviewing PKC ('23, '24), JISA ('23), Financial Cryptography ('24), EUROCRYPT ('25), CRYPTO ('24, '25), ASIACRYPT ('24, '25), CT-RSA ('25), SCN ('26), ESORICS ('26).

Committees Member of the EUROCRYPT'26 local organizing team.

Skills

Languages Italian (native), English (proficiency; self-assessment).

Technical Skills **Programming Languages**: C, Python, Kotlin, C#, Java, Assembly (x86 AT&T), SQL.
Version control: Git · **Smart contracts**: Solidity · **Reverse engineering**: IDA.
Network security: Opnsense, Wireguard · **Android development**: Android Studio.
Typesetting and word processing: TeX, Office Suite.

Driving License Italian Driving License – Patente B.

Talks and Lectures

Conference Talks **Robust Non-Interactive Zero-Knowledge Combiners**.
EUROCRYPT 2026 (Rome, Italy) | ArcticCrypt 2025 (Longyearbyen, Norway).
Key Exchange in the Post-Snowden Era: Universally Composable Subversion-Resilient PAKE.
ASIACRYPT 2024 (Kolkata, India).

Bullet Talks **soundcalc-lean: Formally Verifying a zkVM soundness calculator in Lean4**.
2026 · Ethereum Foundation · Ethproofs#9 (Remote).

Invited Talks **Universally Composable Password-Authenticated Key Exchange in the Post-Snowden Era**.
2023 · Technical University of Denmark (Remote) | The University of Edinburgh (Edinburgh, UK).

Guest Lectures **An Introduction to Secure Multi-Party Computation in the presence of Subversion Attacks**.
2025 · Ethical Hacking · MSc Cybersecurity · Sapienza University (Rome, Italy).
An Introduction to SPDZ.
2021 · Secure Computation · MSc Cybersecurity · Sapienza University (Rome, Italy).

Publications

[c3] **Round-Optimal Subversion-Resilient UC PAKE from Malleable Trapdoor Smooth Projective Hash Functions**.
ASIACRYPT 2026. Behzad Abdolmaleki, Suvradip Chakraborty, Shahram Khazaei, Lorenzo Magliocco, Nahid Roustaeifar, Behzad Vahdani, and Daniele Venturi.

[c2] **Robust Non-Interactive Zero-Knowledge Combiners**.
EUROCRYPT 2026. Michele Ciampi, Lorenzo Magliocco, Daniele Venturi, and Yu Xia.

[c1] **Key Exchange in the Post-Snowden Era: Universally Composable Subversion-Resilient PAKE**.
ASIACRYPT 2024. Suvradip Chakraborty, Lorenzo Magliocco, Bernardo Magri, and Daniele Venturi.

Other Activities

Conferences **Cedarcrypt 2026 - Applied Cryptography Summer School & Conference**.
Organized by Symbolic Software. Hosted in Paphos, Cyprus.

Doctoral Schools **Challenges in building Billion Users Cloud Applications (BUCA'24)**.
Organized by the Department of Informatics of Sapienza University jointly with Google. Hosted in Venice, Italy.
Foundations and Frontiers of Probabilistic Proofs (FoPP'23).
Organized by EPFL. Hosted in Zürich, Switzerland.
13th BIU Winter School in Cryptography on Blockchain Technologies.
Organized by Bar-Ilan University. Hosted in Tel Aviv, Israel.

Miscellaneous Ranked first in the selection process for the PhD in Cybersecurity at Sapienza University of Rome.

References

Available upon request.