

Noemi Terzo

[Website](#) | [LinkedIn](#) | [Google Scholar](#)

Email: noemi.terzo@mpi-sp.org

Professional Experience

Doctoral Researcher in Applied Cryptography Feb 2024 – Present

Max Planck Institute for Security and Privacy – Bochum, Germany

Research interests: Security Analysis of Cryptographic Protocols, Secure Messaging, Post-Quantum Cryptography.

Supervised by Peter Schwabe and Cas Cremers.

Visiting Researcher Nov 2025 – Feb 2026

CISPA Helmholtz Center for Information Security – Saarbrücken, Germany

Hosted by Cas Cremers.

Cybersecurity Engineer Intern May 2023 – Oct 2023

European Space Agency – Darmstadt, Germany

Responsible for the implementation of Post-Quantum Cryptography for ground-to-space communications.

Participated in OPS-SAT satellite mission.

Cybersecurity Engineer Intern Feb 2023 – Apr 2023

C4 Army Command - Italian Armed Forces – Rome, Italy

Developed a P.o.C. for a hybrid digital identity management architecture based on Blockchain.

Education

Ph.D. in Computer Science, Applied Cryptography Feb 2024 – Present

Radboud University

M.Sc. in Computer Engineering, specialization in Cybersecurity Sept 2021 – Dec 2023

Polytechnic University of Turin

- **Grade:** 110/110
- **Thesis:** "Design and in-orbit Demonstration of a Post-Quantum Cryptographic Solution Based on KEMTLS-PDK to Enhance Satellite Communication Security"

B.Sc. in Computer Engineering Sept 2018 – Sept 2021

University of Calabria

- **Grade:** With Honors and Academic Mention
- **Thesis:** "Cybersecurity and Human Factor: Techniques and Tools for Social Engineering"

Publications

Message Injection Attacks Against Signal

Kien Tuong Truong, [Noemi Terzo](#), Kenneth Paterson

USENIX Security '26. To appear.

Formal Security Analysis of the Olvid Messenger

[Noemi Terzo](#), Cas Cremers, Ruben Gonzalez, Peter Schwabe, Yuval Yarom, Zhiyuan Zhang

ACM CCS 2026. To appear.

Talks

Signal Lost (Integrity): The Signal App is More than the Sum of its Protocols

Real World Crypto 2026

Olvid – The Good, the Bad and the Ugly

ZISC Seminar Series at ETH Zurich, 2025

Grants and Awards

CYBERCHALLENGE.IT 2023 – Selected to be part of Polytechnic University of Turin team for the main Cybersecurity Italian training program organized by CINI Cybersecurity National Lab.

START STEM Scholarship 2022 – Financed by Unione Industriali Torino.

5x1000 Award 2022 – Financed by University of Calabria.

Key Skills

Formal Methods: Tamarin Prover, ProVerif

Security: Ghidra, Radare2, GDB, nmap, Wire-shark, BurpSuite, mitmproxy, Aircrack-ng, CAINE, Maltego, Flawfinder, PVS-Studio, Spotbugs, Find-SecBugs, angr

Programming languages: Assembly, Bash, C, Java, Maple, MATLAB, PowerShell, Python, Rust, Simulink, VHDL

Database Technologies: Apache Spark, Hadoop MapReduce, PostgreSQL, SQL, XPath, XQuery

Languages

Italian: native; **English:** full professional proficiency, B2 First certificate