Last updated in Jan 2026

Davide Carnemolla

Catania, Italy | davide.carnemolla@phd.unict.it | herbrant.github.io

linkedin.com/in/davide-carnemolla | github.com/Herbrant

Education

University of Catania, PhD in Cryptography – Catania, Italy 2024 - ongoing

- Supervisor: Prof. Dario Catalano

University of Catania, MS in Computer Science – Catania, Italy 2021 - 2023

- Thesis: Implementation and Performance Analysis of Homomorphic Signature Schemes
- Advisors: Prof. Dario Catalano and Prof. Mario Di Raimondo

University of Catania, BS in Computer Science – Catania, Italy 2017 - 2021

- Thesis: ExamBox NG
- Advisor: Prof. Mario Di Raimondo

Experience

Temporary Research Fellow, University of Catania – Catania, Italy 2023 - 2024

Conducted research activities in the field of Multi-Agent Systems and Internet of Things, focusing on the design and analysis of distributed and intelligent systems. Contributed to research tasks including modeling, experimentation, and technical documentation.

- Supervisor: Prof. Fabrizio Messina

Senior Teaching Assistant, University of Catania – Catania, Italy 2024

Provided tutoring and lab support for undergraduate computer science courses, helping students grasp key concepts and prepare for exams.

- Programming 1

Junior Teaching Assistant, University of Catania – Catania, Italy 2023

Provided tutoring and lab support for undergraduate computer science courses, helping students grasp key concepts and prepare for exams.

- Operating Systems

Junior Teaching Assistant, University of Catania – Catania, Italy 2021 - 2022

Provided tutoring and lab support for undergraduate computer science and mathematics courses, helping students grasp key concepts and prepare for exams.

- Operating Systems
- Internet Security
- Distributed Systems
- Informatics 2

Software Developer, Aucta Cognitio/Verge Technologies – Full Remote 2022

Developed and maintained features for the Sendata platform, a cloud-based data storage and archival solution built on distributed technologies. Worked on backend services and system integration for storage solutions leveraging blockchain networks based on Proof of Spacetime, specifically Filecoin by Protocol Labs, collaborating remotely with cross-functional teams.

High School Teacher, Istituto Polivalente Valdisavoia – Catania, Italy 2021 - 2022
Operating Systems and Networks

Publications

On the (Un) biasability of Existing Verifiable Random Functions 2026
Davide Carnemolla, Dario Catalano, Valentina Frasca, Emanuele Giunta
eprint.iacr.org/2025/2176 (Financial Cryptography and Data Security 2026)

Anamorphic Resistant Encryption: the Good, the Bad and the Ugly 2025
Davide Carnemolla, Dario Catalano, Emanuele Giunta, Francesco Migliaro
eprint.iacr.org/2025/233 (Advances in Cryptology – CRYPTO 2025)

An ecosystem to develop multi-agent systems in real-world IoT applications 2025
Davide Carnemolla, Fabrizio Messina, Corrado Santoro, Federico Fausto Santoro
www.authorea.com/doi/full/10.22541/au.175042803.36556435 (Software: Practice and Experience)

Hermes: a Wireless Communication Interface for Edge Computing 2024
Davide Carnemolla, Fabrizio Messina, Corrado Santoro, Federico Fausto Santoro
ceur-ws.org/Vol-3735/paper_03.pdf (WOA 2024)

Awarded Grants

- Public Good Crypto (Microgrant 2025 Q1)

Reviewing Activities

- Subreviewer for Eurocrypt 2026
- Subreviewer for TCC 2025

Skills

Languages: C/C++, Rust, Python, Go, BASH

Systems and Networks: Linux, VM (KVM/QEMU - libvirt), Docker, Kubernetes, Firewall (iptables/nftables), VPN (OpenVPN, Wireguard), Reverse Proxy (Nginx, Traefik)

Research Areas: Cryptography, Security

Other Skills: LaTeX, Git, Backend Development, Embedded Systems Development

Projects

ExamBox NG

ExamBox NG is a software project designed to support the execution of laboratory exams at the Department of Mathematics and Computer Science, University of Catania. The system enables instructors to generate minimal GNU/Linux images containing all the required tools for an exam and to deploy them in a diskless environment across departmental laboratories using the iPXE protocol. The generated images include built-in security mechanisms to prevent student collaboration and access to unauthorized materials during examinations.
Davide Carnemolla, Mario Di Raimondo

DropTheMark

DropTheMark is a web application for publishing exam results while preserving student privacy. It is currently in use at the Department of Mathematics and Computer Science, University of Catania.
Davide Carnemolla, Mario Di Raimondo