europass Curriculum vitae

PERSONAL INFORMATION

Alessandro Palumbo

Avenue de la Boulaie-CS 47601, 35576, Cesson-Sévigné, France

+39 3933979963

alessandro.palumbo@inria.fr

https://palessumbo.github.io/

https://www.linkedin.com/in/alessandro-palumbo-5b178a12b/

Date of birth 29/04/1993 | Nationality Italian

RESEARCH WORK EXPERIENCE

from A.Y. 2023/2024

Associate Researcher @ IRISA Lab, Inria

SUSHI (SecUrity at the Software-Hardware Interface) team member

Research focus: Hardware Security, Side-Channel Analysis, Side-Channel Attacks

04/2024 – 07/2024

Visiting Researcher @ International Computer Science Institute - University of California, Berkeley

Research work sponsored by NGI Enrichers titled: "Techniques to protect Microprocessor-based Systems against Microarchitectural Side-Channel Attacks". More info here

A.Y. 2022/2023

Assistant Researcher @ Politecnico di Milano – DEIB Department

Research work in EU project SHANNON. Research activity titled: "Design of Integrated Circuits for High-Security Primitive of In-Memory Computing"

04/2018 – 10/2019

Part-time research work with CNIT @ University of Rome Tor Vergata – Electronic Engineering department

Research work in EU projects SESAMO and 5G-PICTURE, POR FESR 2014/2020

TEACHING EXPERIENCE

from A.Y. 2023/2024

Associate Professor @ CentraleSupelec, Université Paris Saclay, Rennes Campus

Associate Professor for "Advanced Computer Networks" course, 2EL6110, Workload (HEE): 60, Master's Degree in Cybersecurity, School of Engineering

A.Y. 2022/2023

Contract Professor @ Politecnico di Milano - Online Bachelor Degree in Digital Engineering

Contract Professor for Logical Networks, INGDIG2-3, 5 CFU

Contract Professor for IT Systems and Services, INGDIG2-3, 10 CFU

Teaching Assistant @ Politecnico di Milano - Bachelor Degree in Biomedical Engineering

Teaching Assistant for Computer Science and Element of Medical Informatics, 085851, 7 CFU, ING-INF/05

A.Y. 2021/2022

Contract Professor @ University of Milano Bicocca, Computer Science Department

Contract Professor for Programming 1, 2122-1-E3101Q105, 2 CFU, INF/01

Teaching Assistant @ University of Rome Tor Vergata, Engineering Departments

Teaching Assistant for Mathematical Analysis I, 8037484, 12 CFU, MAT/05

FUNDING RECEIVED

2025 **AAP Oser - Université Paris-Saclay (France)**

Funding for the development of innovative teaching material. Project: creation of comic-style illustrations to explain microprocessor attacks. Role: technical lead and scientific supervisor. Amount: EUR 5000.

2024 **Allocation d'Installation Scientifique (AIS) - Rennes Métropole (France)**

Funding to support newly recruited researchers in establishing their research activities. Amount: EUR 10000. More info here

2024 **Boost'Mobilité, Funded by the Région Bretagne (France)**

Funding to support researchers aiming to establish collaborations with European researchers for project development. Amount: EUR 1000. More info here

2023 **NGI Enrichers Fellowship Grant, Funded by the European Union's Horizon Europe program**

Project: "Techniques to protect Microprocessors-based Systems against Microarchitectural Side-Channel Attacks". Hosted by the International Computer Science Institute - University of California, Berkeley. Amount: EUR 15000. More info here

PHD STUDENTS HOSTED

Nov. 2024 – Feb. 2025 **"Detection of Hardware Threats in Microprocessors Using Probabilistic Data Structures"**

Student: R. B. Martinez (UC3M). Advisors: P. Reviriego (UPM), D. Larrabeiti (UC3M). Co-Advisors: **A. Palumbo**, R. Salvador (CentraleSupélec)

PHD THESES SUPERVISED

from A.Y. 2025/2026 **"Vulnerability analysis, fault modeling, and countermeasures towards dependable real-time computing in safety-critical drone systems"**

Student: V. Abgrall (CentraleSupélec). Advisor: A. Kritikakou (Inria) Co-Advisors: **A. Palumbo**, R. Salvador (CentraleSupélec), M Traiola (Inria)

from A.Y. 2024/2025 **"Towards Secure FPGA-Accelerated Clouds: Identification, Exploitation and Detection of Remote Side-Channel Leakage Sources"**

Student: E. Quéré. Advisor: L. Bossuet (LHC) Co-Advisors: **A. Palumbo**, R. Salvador (CentraleSupélec), M. M. Real (UBS)

APPRENTICESHIPS SUPERVISED

from A.Y. 2024/2025 **"Toward Secure Multilevel Workstations: Threat Models and Implementation Guidelines"**

Student: C. De Reydet De Vulpillieres. Advisor: S. Dellac (Defenso) Co-Advisors: **A. Palumbo**

EDUCATION

11/2019 – 10/2022 **Ph.D. in Electronic Engineering @ University of Rome Tor Vergata, partly financed by MISE (Italian Ministry of Economic Development)**

Research project title: "Features Analysis of Threats in Microprocessors: Attacks Detection & Mitigation Techniques". Manuscript available here

23/10/2019 **Master Degree in Electronic Engineering for Telecommunication and Multimedia @ University of Rome Tor Vergata**

Sperimental thesis titled: “Development, FPGA Implementation & Performance Analysis of an eBPF-based System”

02/11/2016 **Bachelor Degree in Electronic Engineering @ University of Rome Tor Vergata**

Sperimental thesis titled: “Development and FPGA Implementation of an Hardware Module for Encapsulating & Decapsuling Ethernet Packets"

PUBLICATIONS

[1] R. B. Martínez, **A. Palumbo**, et al. “LAD-IXoC: Loop-based Attack Detection with Integrated XOR Filter and CMS”. In: *38th IEEE International Conference on Dependable and Fault Tolerant Systems (DFTS)*. 2025.

[2] **A. Palumbo** and R. Salvador. “Detecting Hardware Trojans in Microprocessors via Hardware Error Correction Code-based Modules”. In: *31st IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS)*. Naples, Italy, 2025.

[3] **A. Palumbo** and R. Salvador. “Leveraging gem5 for Hardware Trojan Research: Simulation for Machine-Learning-Based Detection”. In: *3rd International Workshop on Malware in the Internet of Things (Mal-IoT ’25)*. Cagliari, Italy: ACM, May 2025.

[4] G. Garzo and **A. Palumbo**. “Legal & Ethical Implications of Predictive Digital Techniques in the Judicial Criminal Proceedings”. In: *13th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE. Boston, MA, USA: IEEE, 2025.

[5] G. Garzo and **A. Palumbo**. “Human-in-the-Loop: Legal Knowledge Formalization in Attempto Controlled English”. In: *13th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE. Boston, MA, USA: IEEE, 2025.

[6] G. Garzo and **A. Palumbo**. “The First Hardware Circuit Emulating Italian Road Homicides Legal Logic, DAJE!” In: *23rd IADIS International Conference on e-Society*. Accepted for publication. Lisbon, Portugal: IADIS, Mar. 2025.

[7] G. Garzo, S. Ribes, and **A. Palumbo**. “Opening the Black Box: How Boolean AI can Support Legal Analysis”. In: *4th IEEE International Conference on Computer Communication and Artificial Intelligence (CCAI)*. 2024.

[8] S. Ribes, F. Malatesta, G. Garzo, and **A. Palumbo**. “Machine Learning-Based Classification of Hardware Trojans in FPGAs Implementing RISC-V Cores”. In: *10th International Conference on Information System Security and Privacy*. 2024.

[9] **A. Palumbo** et al. “Built-in Software Obfuscation for Protecting Microprocessors against Hardware Trojan Horses”. In: *36th IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*. 2023, pp. 1–6.

[10] **A. Palumbo** et al. “Improving the Detection of Hardware Trojan Horses in Microprocessors via Hamming Codes”. In: *36th IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*. 2023.

[11] P. R. Nikiema, **A. Palumbo**, et al. “Towards Dependable RISC-V Cores for Edge Computing Devices”. In: *29th IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS)*. 2023.

[12] M. S. Brunella, G. Belocchi, M. Bonola, S. Pontarelli, G. Siracusano, G. Bianchi, A. Cammarano, **A. Palumbo**, L. Petrucci, and R. Bifulco. “hXDP: Efficient software packet processing on FPGA NICs”. In: *Communications of the ACM* 65.8 (2022).

[13] L. Cassano, S. Di Mascio, **A. Palumbo**, A. Menicucci, G. Furano, G. Bianchi, and M. Ottavi. “Is RISC-V ready for Space? A Security Perspective”. In: *35th IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*. 2022.

[14] **A. Palumbo**, K. Arıkan, et al. “Processor Security: Detecting Microarchitectural Attacks via Count-Min Sketches”. In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2022), pp. 1–14.

[15] **A. Palumbo** et al. “Is your FPGA bitstream Hardware Trojan-free? Machine learning can provide an answer”. In: *Journal of Systems Architecture* (2022), p. 102543.

[16] **A. Palumbo** et al. “A Lightweight Security Checking Module to Protect Microprocessors against Hardware Trojan Horses”. In: *34th IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*. IEEE. 2021.

[17] M. S. Brunella, G. Belocchi, M. Bonola, S. Pontarelli, G. Siracusano, G. Bianchi, A. Cammarano, **A. Palumbo**, L. Petrucci, and R. Bifulco. “hXDP: Efficient Software Packet Processing on {FPGA} NICs”. In: *14th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 20),* ***Best Paper Award***. 2020.

[18] **A. Palumbo** et al. “Nuovi approcci per garantire la sicurezza nei sistemi hardware.” In: *LA COMUNICAZIONE Note Recensioni e Notizie, Volume LXIII*. 2020, pp. 98–117.