Francesco Antognazza

via Togliatti 3, 22070 Carbonate, Italy
+39 02 2399 9047
francesco.antognazza@polimi.it
https://antognazza.faculty.polimi.it/
ORCID 0000-0003-3480-486X

Education and qualifications

2020-now **Ph.D. in Information Technology**, *Politecnico di Milano*, Post-quantum cryptographic accelerators for the Internet of Things applications.
Supervisors: Gerardo Pelosi, Alessandro Barenghi

2017-2020 **Master of Computer Science**, *Politecnico di Milano*, Countering side channel attacks in an in-order RISC-V processor with a code morphing based execution mode
Supervisors: Gerardo Pelosi, Alessandro Barenghi

2014-2017 **Bachelor of Computer Science**, *Politecnico di Milano*

Research skills and experiences

Digital systems design — Analysis, development, optimization, and validation of RTL hardware accelerators for NTRU and HQC asymmetric cryptographic schemes from the NIST Post-Quantum Cryptography (PQC) standardization process

HW/SW co-design — HW/SW co-design, development, and testing of a RISC-V microcontroller extending the OpenTitan SoC project through a novel instruction decode stage to apply a countermeasure against a power-based side-channel attack, which in turn realizes a run-time replacement of a sensitive instruction with a sequence of semantically equivalent protected instructions

Side-channel analysis — Execution of side-channel attacks on hardware and software implementations of cryptographic algorithms, and implementation of countermeasures to mitigate the information leakage

SW optimization — Benchmarking software for embedded devices, and code optimization for a specific target architecture

Grants and awards

Ph.D. Scholarship — **ST Microelectronics (Nov. 2020 - Oct. 2023)**, *collaboration with the R&D personnel of the cryptography and computer security division on the topic "Hardware Implementation of Post-Quantum Cryptographic Algorithms for the IoT"*

Award — **Nominee for Best Student Paper**, *An Efficient Unified Architecture for Polynomial Multiplications in Lattice-Based Cryptoschemes*, 9th International Conference on Information Systems Security and Privacy, ICISSP 2023, Lisbon, Portugal, February 22-24, 2023

Award — **Best Student Poster**, *A Versatile and Unified HQC Hardware Accelerator*, 22nd International Applied Cryptography and Network Security Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5-8, 2024

Teaching experience

2021-2023 **Computer architecture and operating systems**, *Teaching Assistant*, Politecnico di Milano, A.Y. 2021-2022 (34 hours), A.Y. 2022-2023 (40 hours), A.Y. 2023-2024 (20 hours)

Languages

Italian — Mother tongue

English — B2 — *TOEIC certification (August 2017): 900/990*

Other

Summer school — **17th International Summer School on Advanced Computer Architecture and Compilation for High-performance Embedded Systems**, *Fiuggi, Italy, September 12-18, 2021*, Presenter at the poster session "Metis: An Integrated Morphing Engine CPU to Protect Against Side Channel Attacks"

Summer school — **Real-world crypto and privacy**, *Šibenik, Croatia, June 13-17, 2022*

Summer school — **Post-Quantum Cryptography 2022**, *Budapest, Hungary, August 1-5, 2022*

Peer-review — Sub-reviewer for IEEE Transactions on Information Forensics and Security (TIFS), IEEE Access, International Conference on Computer-Aided Design (ICCAD) 2021-2022, Design Automation and Test in Europe (DATE) 2024, International Conference on Cryptology And Network Security (CANS) 2021

Referees

Gerardo Pelosi, *Associate Professor*, Politecnico di Milano, (MI) Italy
gerardo.pelosi@polimi.it `https://pelosi.faculty.polimi.it/doku.php`

Alessandro Barenghi, *Associate Professor*, Politecnico di Milano, (MI) Italy
alessandro.barenghi@polimi.it `https://barenghi.faculty.polimi.it/doku.php`

Publication list

F. Antognazza, A. Barenghi, and G. Pelosi, "Metis: An integrated morphing engine CPU to protect against side channel attacks," *IEEE Access*, vol. 9, pp. 69210–69225, 2021, DOI:10.1109/ACCESS.2021.3077977.

F. Antognazza, A. Barenghi, G. Pelosi, and R. Susella, "A flexible asic-oriented design for a full NTRU accelerator," in *Proceedings of the 28th Asia and South Pacific Design Automation Conference, ASPDAC 2023, Tokyo, Japan, January 16-19, 2023* (A. Takahashi, ed.), pp. 591–597, ACM, 2023, DOI:10.1145/3566097.3567916.

F. Antognazza, A. Barenghi, G. Pelosi, and R. Susella, "An efficient unified architecture for polynomial multiplications in lattice-based cryptoschemes," in *Proceedings of the 9th International Conference on Information Systems Security and Privacy, ICISSP 2023, Lisbon, Portugal, February 22-24, 2023* (P. Mori, G. Lenzini, and S. Furnell, eds.), pp. 81–88, SciTePress, 2023, DOI:10.5220/0011654200003405.

F. Antognazza, A. Barenghi, G. Pelosi, and R. Susella, "Performance and efficiency exploration of hardware polynomial multipliers for post-quantum lattice-based cryptosystems," *SN Comput. Sci.*, vol. 5, no. 2, p. 212, 2024, DOI:10.1007/S42979-023-02547-W.

F. Antognazza, A. Barenghi, G. Pelosi, and R. Susella, "A versatile and unified HQC hardware accelerator," in *Applied Cryptography and Network Security - 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5-8, 2024, Proceedings*, Lecture Notes in Computer Science, Springer, 2024, To Appear.

F. Antognazza, A. Barenghi, G. Pelosi, and R. Susella, "A high efficiency hardware design for the post-quantum KEM HQC," in *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2024, Washington, DC, USA, May 6-9, 2024*, IEEE, 2024, To Appear.

Milan, March 27th, 2024

Yours faithfully
Francesco Antognazza

I authorize the processing of personal data in this document in compliance with privacy regulations.