Francesco Antognazza

✉ *francesco.antognazza@polimi.it*
🌐 *https://antognazza.faculty.polimi.it/*
ORCID 0000-0003-3480-486X

Education and qualifications

2020-2025 **Ph.D. in Information Technology**, *Politecnico di Milano*,
Hardware Design and Implementation of Post-Quantum Cryptographic Algorithms: the case of NTRU, HQC and CROSS
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 efficient RTL hardware accelerators using SystemVerilog for NTRU, HQC and CROSS asymmetric cryptographic schemes from the NIST Post-Quantum Cryptography (PQC) standardization process, along with many other auxiliary components such as Hash Functions (SHA-2, SHA-3), stream ciphers (ChaCha20), and Pseudo Random Number Generators.

Design Space Exploration — Development of highly parametrized modules with different trade-off points between latency and area leveraging the algorithmic properties, determining the Pareto optimal points with the highest efficiency via automated benchmarking toolchains.

HW Design Generalization — Enabling cryptographic agility by leveraging algebraic properties to generalize hardware designs, enabling efficient reuse of hardware modules to support similar algorithms in a single design.

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 random sequence of semantically equivalent instructions.

Side-Channel Analysis — Assessment of EM side-channel leakage on hardware and software implementations of cryptographic algorithms, and implementation of countermeasures to mitigate the information leakage.

Software Engineering — Application of Software Engineering best practices to enable reproducible builds and Continuous Verification via container technology and open-source tools, and leveraging CPU parallelism for rapid Design Space Exploration.

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"*

Nominee — **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

2021-2025 **Computer architecture and operating systems**, *Teaching Assistant*, Politecnico di Milano, 115 hours – A.Y. 2021-2025

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, Design Automation and Test in Europe (DATE) 2024, European Symposium on Research in Computer Security (ESORICS) 2024, International Conference on Computer-Aided Design (ICCAD) 2021-2022, International Conference on Cryptology And Network Security (CANS) 2021, International Workshop on Code-Based Cryptography (CBCrypto) 2024

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, pp. 214–219, Springer, 2024.

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, Tysons Corner, VA, USA, May 6-9, 2024*, pp. 431–441, IEEE, 2024.

F. Antognazza, A. Barenghi, and G. Pelosi, “An efficient and unified rtl accelerator design for hqc-128, hqc-192, and hqc-256,” *IEEE Transactions on Computers*, pp. 1–14, 2025.

Milan, Thursday 22th, 2025

Yours faithfully
Francesco Antognazza

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