Ph.D. in Information Technology
Thesis Defense

May 22th, 2025
at 11:00 am
Room Beta – building 24

Francesco Antognazza – XXXVI Cycle

Hardware Design and Implementation of Post-Quantum Cryptographic Algorithms: the case of NTRU, HQC and CROSS

Supervisor: Prof. Gerardo Pelosi
Co-supervisor: Prof. Alessandro Barenghi

Abstract:

During the last decade, public key cryptography received renewed attention from academic, industrial and institutional stakeholders due to the consistent advancements in the development of more capable quantum computers, which are deemed able to break in the near future the security guarantees provided by the currently deployed cryptographic algorithms based on the hardness of the integer factorization or discrete logarithm problems (e.g., RSA and ECC) thanks to Shor's algorithm. In 2016, the U.S.A. National Institute of Standards and Technology published a call for public key schemes resistant to quantum-computer-aided attacks, intending to replace the vulnerable algorithms currently in use and asking the community for cryptanalysis and optimized software and hardware implementations of the proposals. After several rounds of selection, schemes based on lattices and forward error-correction codes proved to be the most promising. Taking a hardware design perspective, I focused on analyzing the key encapsulation mechanism based on the Hoffstein, Pipher, and Silverman's NTRUEncrypt encryption scheme, commonly referred to as NTRU, the key encapsulation mechanism named "Hamming Quasi-Cyclic" (HQC), and the digital signature algorithm named "Codes and Restricted Objects Signature Scheme" (CROSS), with a particular emphasis on the optimization of the latency and the efficiency of their building blocks such as polynomial multipliers, random polynomial samplers and encoders/decoders for the Reed-Muller/Reed-Solomon concatenated code, ideating and comparing novel specialized algorithms for the sub-procedures composing the cryptoschemes and providing results for both FPGA and ASIC design flows. The results show a substantially improved latency and efficiency compared to the state-of-the-art, and a proposed algorithmic optimization for HQC was recently included in the official specification.

PhD Committee

Prof. Giovanni Agosta, Politecnico di Milano

Prof. Guido Masera, Politecnico di Torino

Prof. Francesco Regazzoni, University of Amsterdam