POLITECNICO DI MILANO

PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 41st cycle

Research Area n. 1 - Computer Science and Engineering

ACN - CYBER Research Field: DESIGN OPTIMIZATION AND SIDE-CHANNEL ANALYSES OF POST-QUANTUM CODE-BASED CRYPTOSYSTEMS

Monthly net income of PhDscholarship (max 36 months)
1600.0 In case of a change of the welfare rates during the three-year period, the amount could be modified.

Context of the research activity	
Motivation and objectives of the research in this field	The protection against side channel attacks of recently introduced post-quantum cryptoschemes is recognized as a primary objective for ensuring the confidentiality and authentication capabilities of quantum-ready protocols and applications running on real-world devices. The transition of current cryptographic technologies towards post-quantum methods is recommended by a large number of EU and US institutional bodies. This transition is necessary to effectively prevent the "harvest-now-decrypt-later" threats arising from the rapid development of quantum computing technologies. Theoretical security models applied in the design of post quantum cryptosystems do not adequately address the degree of protection that an actual implementation of these systems can provide. Consequently, there is a recognized gap in related academic and industrial research studies that motivates investigating possible security weaknesses in the software and hardware implementations of post-quantum cryptosystems on several computing platforms, as well as designing related countermeasures. Objectives of the study will be a side channel assessment of code-based post-quantum cryptoschemes; the development, testing and possible automated application of countermeasures already known to be effective against specific attacks, as well as the investigations and the

	design of new countermeasures based on the theory of “non-malleable” codes.
Methods and techniques that will be developed and used to carry out the research	Side channel analyses (SCA) can be categorized into two distinct classifications: active (or fault-based) attacks and passive attacks. The distinction between these two categories is determined by the extent of tampering permitted by the attacker. In active attacks, the attacker is permitted to directly manipulate the computing device, while in passive attacks, the attacker's intervention is limited to the measurement of environmental parameters during the computation. Research activities on passive SCA against software implementations of post-quantum cryptosystems (running on several platforms, among which the ARM microcontrollers) will entail the utilization of specialized equipment for the measurement of side channel signals across diverse computing platforms, including ARM microcontrollers. These signals will then be processed to extract the features necessary for executing the most effective attacks at the state of the art. These attacks include vertical, horizontal, template, and machine learning-based methods. The research activities will focus also on the application of known countermeasures (such as masking, shuffling, random delay insertion, and code polymorphism) and the possibility of automating it. The project will also consider the perspective of modifying components of some of the currently most promising code-based schemes. These include LESS, CROSS, and HQC, which are currently either selected for standardization or runners-up. The goal of this modification will be to replace some of their SCAs vulnerable operations with others that do not exhibit sensitive information leakage. Finally, a further line of investigation will address the theory and development of "non-malleable codes" to ensure the security of code based post-quantum schemes against fault induction-based SCAs. To such a purpose the main case study will be the, recently standardized, HQC key encapsulation method.
Educational objectives	Key educational objectives include understanding the theoretical foundations of code-based post-quantum

	cryptosystems (PQC), evaluating existing schemes like those from the NIST PQC competition, designing software solutions for real-world deployment, ensuring resilience against side-channel attacks, and facilitating the integration of these new cryptographic standards into existing protocols and infrastructures.
Job opportunities	Opportunities for experts in cryptography and side-channel analysis exist in sectors like: academia, government agencies, technology companies developing secure systems, consulting firms specialized in computer security and cryptography. Roles/Job titles: Applied Cryptographer, Cryptography Security Analyst, Research Scientist, Security Engineer, Software Engineer, Investigation Specialist.
Composition of the research group	0 Full Professors 2 Associated Professors 2 Assistant Professors 3 PhD Students
Name of the research directors	Prof. Gerardo Pelosi

Contacts
gerardo.pelosi@polimi.it

Additional support - Financial aid per PhD student per year (gross amount)	
Housing - Foreign Students	--
Housing - Out-of-town residents	--

Scholarship Increase for a period abroad	
Amount monthly	800.0 €
By number of months	6

Additional information: educational activity, teaching assistantship, computer availability, desk availability, any other information
Additional information: educational activity, teaching assistantship, computer availability, desk availability, any other information. EDUCATIONAL ACTIVITIES (purchase of study books and material, including computers, funding for participation in courses, summer schools, workshops and conferences): financial aid per PhD student.

TEACHING ASSISTANTSHIP: availability of funding in recognition of supporting teaching activities by the PhD student. There are various forms of financial aid for activities of support to the teaching practice.
The PhD student is encouraged to take part in these activities, within the limits allowed by the regulations.

COMPUTER AVAILABILITY:
1st year: Yes
2nd year:Yes
3rd year: Yes